Scan Report

June 28, 2021

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "192.168.0.116". The scan started at Mon Jun 28 04:07:22 2021 UTC and ended at Mon Jun 28 04:21:03 2021 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.0.116	0	4	0	16	0
Total: 1	0	4	0	16	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Debug" are not shown.

This report contains all 20 results selected by the filtering described above. Before filtering there were 20 results.

2 Results per Host

2.1 192.168.0.116

Host scan start	Mon Jun 28 04:07:54 2021 UTC
Host scan end	Mon Jun 28 04:20:59 2021 UTC

Service (Port)	Threat Level
22/tcp	Medium
general/tcp	Medium
22/tcp	Log
general/CPE-T	Log
22222/tcp	Log
111/tcp	Log
general/tcp	Log
3389/tcp	Log

2.1.1 Medium 22/tcp

Medium (CVSS: 6.8)
NVT: OpenSSH <= 8.3p1 Command Injection Vulnerability

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)`

. . . continues on next page . . .

... continued from previous page ...

Summary
OpenSSH is prone to a remote code execution vulnerability.

Vulnerability Detection Result
`Installed version: 7.6p1`
`Fixed version: None Available`
`Installation path / port: 22/tcp`

Impact
Successful exploitation would allow an attacker to execute arbitrary code on the target machine.

Solution:
Solution type: NoneAvailable
No known solution is available as of 29th January, 2021. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH through version 8.3p1.

Vulnerability Insight
scp of OpenSSH allows command injection in spc.c via backtick characters in the destination argument.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH <= 8.3p1 Command Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113736
Version used: `2021-01-29T09:14:09Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
`cve: CVE-2020-15778`
`url: https://github.com/cpandya2909/CVE-2020-15778/`
`dfn-cert: DFN-CERT-2020-1691`

Medium (CVSS: 5.3)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Linux

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: None
Installation
path / port: 22/tcp

Impact
Successfully exploitation will allow a remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
OpenSSH version 5.9 through 7.8.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Linux
OID:1.3.6.1.4.1.25623.1.0.813888
Version used: 2021-05-28T07:06:21Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
cve: CVE-2018-15919

... continues on next page ...

... continued from previous page ...

url: https://bugzilla.novell.com/show_bug.cgi?id=1106163
url: https://seclists.org/oss-sec/2018/q3/180
cert-bund: CB-K18/0885
dfn-cert: DFN-CERT-2018-2293
dfn-cert: DFN-CERT-2018-2191

Medium (CVSS: 5.3)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: 7.8
Installation
path / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution:
Solution type: VendorFix
Update to version 7.8 or later.

Affected Software/OS
OpenSSH versions 7.7 and prior on Linux

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)
OID:1.3.6.1.4.1.25623.1.0.813864
Version used: 2021-05-28T04:00:18Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
cve: CVE-2018-15473
url: https://0day.city/cve-2018-15473.html
url: https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d
↪1e0
cert-bund: CB-K20/0041
cert-bund: CB-K18/1031
cert-bund: CB-K18/0873
dfn-cert: DFN-CERT-2020-2189
dfn-cert: DFN-CERT-2020-0228
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-0857
dfn-cert: DFN-CERT-2019-0362
dfn-cert: DFN-CERT-2018-2293
dfn-cert: DFN-CERT-2018-2259
dfn-cert: DFN-CERT-2018-2191
dfn-cert: DFN-CERT-2018-1806
dfn-cert: DFN-CERT-2018-1696

[return to 192.168.0.116]

2.1.2 Medium general/tcp

Medium (CVSS: 5.0)
NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability

Summary
The host is running TCP services and is prone to denial of service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

Solution:
Solution type: VendorFix
Please see the referenced advisories for more information on obtaining and applying fixes.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
The TCP/IP v4 stack of various products / vendors including:
- Microsoft Windows
- Cisco
- Juniper JunOS

Vulnerability Insight
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

Vulnerability Detection Method
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not.
Note: At least one open TCP port needs to be available and detected at the target host for this vulnerability check.
Details: `TCP Sequence Number Approximation Reset Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902815
Version used: `2020-08-24T08:40:10Z`

References
`cve: CVE-2004-0230`
`bid: 10183`
`url: http://xforce.iss.net/xforce/xfdb/15886`
`url: https://www.us-cert.gov/ncas/archives/alerts/TA04-111A`
`url: http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949`
`url: http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950`
`url: http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006`
`url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2005/ms`
`↪05-019`
`url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2006/ms`
`↪06-064`
`url: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco`
`↪-sa-20040420-tcp-nonios`
`cert-bund: CB-K17/0697`
`cert-bund: CB-K17/0297`
`cert-bund: CB-K17/0238`
`cert-bund: CB-K17/0168`
`cert-bund: CB-K15/0080`
`cert-bund: CB-K14/1162`
`cert-bund: CB-K14/0852`
`dfn-cert: DFN-CERT-2020-1087`
`dfn-cert: DFN-CERT-2017-0719`
`dfn-cert: DFN-CERT-2017-0305`
`dfn-cert: DFN-CERT-2017-0249`
`dfn-cert: DFN-CERT-2017-0171`
`dfn-cert: DFN-CERT-2015-0082`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2014-1217
dfn-cert: DFN-CERT-2014-0890
```

[return to 192.168.0.116]

2.1.3 Log 22/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`An ssh server is running on this port`

Solution:

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

Log (CVSS: 0.0)
NVT: SSH Server type and version

Summary
This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result

```
Remote SSH server banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Remote SSH supported authentication: password,publickey
Remote SSH text/login banner: (not available)
This is probably:
- OpenSSH
Concluded from remote connection attempt with credentials:
Login:    OpenVASVT
Password: OpenVASVT
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: SSH Server type and version
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: 2021-06-21T07:41:28Z

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms are supported by the remote SSH Service.

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffi
↪e-hellman-group14-sha1
server_host_key_algorithms:
ssh-rsa,rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
mac_algorithms_server_to_client:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Solution:

Log Method
Details: SSH Protocol Algorithms Supported

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105565
Version used: 2020-08-24T08:40:10Z

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result
```
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: c7:e5:68:a5:0f:32:3e:4b:b2:9b:df:3f:8f:93:84:e3
ssh-ed25519: 14:c9:dc:38:df:b1:b2:c8:1c:ce:4f:c2:a8:55:96:ee
ssh-rsa: 54:3e:33:56:d8:ab:cd:16:36:cf:f8:cc:66:70:38:1f
```

Solution:

Log Method
Details: SSH Protocol Versions Supported
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: 2020-08-24T08:40:10Z

[return to 192.168.0.116]

2.1.4 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.
Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

Vulnerability Detection Result
```
192.168.0.116|cpe:/a:openbsd:openssh:7.6p1
192.168.0.116|cpe:/o:canonical:ubuntu_linux:18.04
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: 2021-04-16T10:39:13Z

References
url: https://nvd.nist.gov/products/cpe

[return to 192.168.0.116]

2.1.5 Log 22222/tcp

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result
The following certificate details of the remote service were collected.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#626F6B796F756E672E6B75406C67652E636F6D,CN=Tea
↪m2,OU=Security Specialist,O=LG Electronics,L=Seoul,ST=Seoul,C=KR
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#626F6B796F756E672E6B75406C67652E636F6D,CN=CA
↪for Team2,OU=Security Specialist,O=LG Electronics,L=Seoul,ST=Seoul,C=KR
serial ....: 6604203EE8CDC099326715AA79AE5BBF9AD5F6D2
valid from : 2021-06-09 09:29:47 UTC
valid until: 2031-06-07 09:29:47 UTC
fingerprint (SHA-1): CED271167142792FCB4A7DE28580A2731FD6A6E9
fingerprint (SHA-256): BA79A8381115D1C3F6EE5A5980ECBFFC4C039634EB0DFA67B7949B005
↪2E5D1F7

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2021-04-16T08:08:22Z

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result
`This port was detected as being open by a port scanner but is now closed.`
`This service might have been crashed by a port scanner or by a plugin`

Solution:

Log Method
Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `2019-02-20T11:12:24Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A TLScustom server answered on this port`

Solution:

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

[return to 192.168.0.116]

2.1.6 Log 111/tcp

Log (CVSS: 0.0)
NVT: RPC Portmapper Service Detection (TCP)

Summary
TCP based detection of a RPC portmapper service.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
A RPC portmapper service is running on this port.

Solution:

Log Method
Details: RPC Portmapper Service Detection (TCP)
OID:1.3.6.1.4.1.25623.1.0.108090
Version used: 2021-04-14T09:28:27Z

Log (CVSS: 0.0)
NVT: Obtain list of all port mapper registered programs via RPC

Summary
This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Vulnerability Detection Result
```
These are the registered RPC programs:
RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/TCP
RPC program #100227 version 3 'nfs_acl' on port 2049/TCP
RPC program #100005 version 1 'mountd' (mount showmount) on port 33839/TCP
RPC program #100021 version 1 'nlockmgr' on port 39809/TCP
RPC program #100021 version 3 'nlockmgr' on port 39809/TCP
RPC program #100021 version 4 'nlockmgr' on port 39809/TCP
RPC program #100005 version 2 'mountd' (mount showmount) on port 43587/TCP
RPC program #100005 version 3 'mountd' (mount showmount) on port 57713/TCP
RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/UDP
RPC program #100227 version 3 'nfs_acl' on port 2049/UDP
RPC program #100005 version 3 'mountd' (mount showmount) on port 37003/UDP
RPC program #100021 version 1 'nlockmgr' on port 39056/UDP
RPC program #100021 version 3 'nlockmgr' on port 39056/UDP
RPC program #100021 version 4 'nlockmgr' on port 39056/UDP
RPC program #100005 version 2 'mountd' (mount showmount) on port 58553/UDP
```

... continues on next page ...

... continued from previous page ...

RPC program #100005 version 1 'mountd' (mount showmount) on port 59813/UDP

Solution:

Log Method
Details: Obtain list of all port mapper registered programs via RPC
OID:1.3.6.1.4.1.25623.1.0.11111
Version used: 2021-04-14T09:28:27Z

[return to 192.168.0.116]

2.1.7 Log general/tcp

Log (CVSS: 0.0)
NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Vulnerability Detection Result
Network route from scanner (10.0.2.15) to target (192.168.0.116):
10.0.2.15
192.168.0.116
Network distance between scanner and target: 2

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: 2021-03-12T14:25:59Z

Log (CVSS: 0.0)
NVT: OpenSSH Detection Consolidation

Summary

... continues on next page ...

... continued from previous page ...

The script reports a detected OpenSSH including the version number.

Vulnerability Detection Result

```
Detected OpenSSH Server
Version:       7.6p1
Location:      22/tcp
CPE:           cpe:/a:openbsd:openssh:7.6p1
Concluded from version/product identification result:
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
```

Solution:

Log Method

Details: `OpenSSH Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.108577
Version used: `2019-05-23T06:42:35Z`

References

`url: https://www.openssh.com/`

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary

This script consolidates the OS information detected by several VTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result

```
Best matching OS:
OS:            Ubuntu 18.04
Version:       18.04
CPE:           cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (Operating System (OS) Detection (SSH
↪))
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.
↪3
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS:            Linux/Unix
CPE:           cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.100062 (Microsoft Remote Desktop Protocol (R
↪DP) Detection)
```

... continues on next page ...

... continued from previous page ...

Concluded from Microsoft Remote Desktop Protocol (RDP) on port 3389/tcp: Unixoid
↪e based on binary response fingerprinting: 030000130ed000001234000201080000000
↪000

Solution:

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2021-06-24T10:13:15Z

References
url: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Vulnerability Detection Result
Hostname determination for IP 192.168.0.116:
Hostname|Source
192.168.0.116|IP-address

Solution:

Log Method
Details: Hostname Determination Reporting
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: 2018-11-19T11:11:31Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Vulnerability Detection Result
The following additional but not resolvable hostnames were detected:
Team2

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: `SSL/TLS: Hostname discovery from server certificate`
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: `2020-11-10T15:30:28Z`

[return to 192.168.0.116]

2.1.8 Log 3389/tcp

Log (CVSS: 0.0)
NVT: Microsoft Remote Desktop Protocol (RDP) Detection

Summary
A service supporting the Microsoft Remote Desktop Protocol (RDP) is running at this host.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution:

Vulnerability Insight
Remote Desktop Services, formerly known as Terminal Services, is one of the components of Microsoft Windows (both server and client versions) that allows a user to access applications and data on a remote computer over a network.

Log Method
Details: `Microsoft Remote Desktop Protocol (RDP) Detection`
OID:1.3.6.1.4.1.25623.1.0.100062
Version used: `2021-04-16T08:08:22Z`

[return to 192.168.0.116]