BRIDGE TECHNOLOGIES™

***Product:***
VB330 (CentOS7-based_6.1)

***Date performed:***
23.5.2022, 13:09

# RESULTS OF SECURITY AUDIT

Below is a brief overview of results from the audit. For more details, please see the corresponding attachments.

| Description | |
|---|---|
| Vulnerability scan (GVM/OpenVAS) | **OK** |

## Remarks

- TCP timestamps: on legacy Linux-kernels this will leak information about uptime. Is required for some saturation-related TCP-mechanisms to work, and performance will be negatively affected without it. As such, it is not considered a security concern.

# Scan Report

June 7, 2022

**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 "test triggered scan". The scan started at Tue Jun 7 10:57:17 2022 UTC and ended at Tue Jun 7 11:11:17 2022 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** **2**

1.1 Host Authentications . . . . . 2

**2 Results per Host** **2**

2.1 10.0.28.140 . . . . . 2

2.1.1 High general/tcp . . . . . 3

2.1.2 Medium general/tcp . . . . . 7

2.1.3 Log general/tcp . . . . . 11

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 10.0.28.140<br>hw86-aa87.btech.tv | 4 | 2 | 0 | 4 | 0 |
| Total: 1 | 4 | 2 | 0 | 4 | 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 "High" are not shown.
Issues with the threat level "Medium" are not shown.
Issues with the threat level "Low" are not shown.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains results 1 to 10 of the 121 results selected by the filtering described above. Before filtering there were 432 results.

## 1.1 Host Authentications

| Host | Protocol | Result | Port/User |
|---|---|---|---|
| 10.0.28.140 - hw86-aa87.btech.tv | SSH | Success | Protocol SSH, Port 22, User root |
| 10.0.28.140 - hw86-aa87.btech.tv | SSH | Success | Protocol SSH, Port 22, User root |

# 2 Results per Host

## 2.1 10.0.28.140

| | |
|---|---|
| Host scan start | Tue Jun 7 10:57:36 2022 UTC |
| Host scan end | Tue Jun 7 11:11:11 2022 UTC |

| Service (Port) | Threat Level |
|---|---|
| general/tcp | High |
| general/tcp | Medium |
| general/tcp | Log |

### 2.1.1 High general/tcp

High (CVSS: 7.5)
NVT: CentOS: Security Advisory for bind (CESA-2020:5011)

**Summary**
The remote host is missing an update for the 'bind' package(s) announced via the CESA-2020:5011 advisory.

**Vulnerability Detection Result**
`Vulnerable package: bind-export-libs`
`Installed version: bind-export-libs-9.11.4-26.P2.el7`
`Fixed version: bind-export-libs-9.11.4-26.P2.el7_9.2`

**Solution:**
**Solution type:** VendorFix
Please install the updated package(s).

**Affected Software/OS**
'bind' package(s) on CentOS 7.

**Vulnerability Insight**
The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named), a resolver library (routines for applications to use when interfacing with DNS), and tools for verifying that the DNS server is operating correctly.
Security Fix(es):
bind: truncated TSIG response can lead to an assertion failure (CVE-2020-8622)
bind: remotely triggerable assertion failure in pk11.c (CVE-2020-8623)
bind: incorrect enforcement of update-policy rules of type 'subdomain' (CVE-2020-8624)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
Bug Fix(es):
BIND stops DNSKEY lookup in get_dst_key() when a key with unsupported algorithm is found first [RHEL7] (BZ#1884530)

**Vulnerability Detection Method**
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bind (CESA-2020:5011)`
OID:1.3.6.1.4.1.25623.1.0.883292
Version used: `2021-07-06T02:00:40Z`

**References**
`cve: CVE-2020-8622`
`cve: CVE-2020-8623`
`cve: CVE-2020-8624`

... continues on next page ...

... continued from previous page ...

```
cesa: 2020:5011
url: https://lists.centos.org/pipermail/centos-announce/2020-November/035850.htm
↪l
cert-bund: CB-K21/0337
cert-bund: CB-K20/1253
cert-bund: CB-K20/1030
cert-bund: CB-K20/0837
dfn-cert: DFN-CERT-2021-0955
dfn-cert: DFN-CERT-2021-0924
dfn-cert: DFN-CERT-2021-0776
dfn-cert: DFN-CERT-2020-2588
dfn-cert: DFN-CERT-2020-2205
dfn-cert: DFN-CERT-2020-2064
dfn-cert: DFN-CERT-2020-1886
dfn-cert: DFN-CERT-2020-1875
dfn-cert: DFN-CERT-2020-1835
```

High (CVSS: 8.1)
NVT: CentOS: Security Advisory for bind (CESA-2021:0671)

**Summary**
The remote host is missing an update for the 'bind' package(s) announced via the CESA-2021:0671 advisory.

**Vulnerability Detection Result**

```
Vulnerable package: bind-export-libs
Installed version:  bind-export-libs-9.11.4-26.P2.el7
Fixed version:      bind-export-libs-9.11.4-26.P2.el7_9.4
```

**Solution:**
**Solution type:** VendorFix
Please install the updated package(s).

**Affected Software/OS**
'bind' package(s) on CentOS 7.

**Vulnerability Insight**
The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named), a resolver library (routines for applications to use when interfacing with DNS), and tools for verifying that the DNS server is operating correctly.
Security Fix(es):
bind: Buffer overflow in the SPNEGO implementation affecting GSSAPI security policy negotiation (CVE-2020-8625)

... continues on next page ...

... continued from previous page ...

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

**Vulnerability Detection Method**
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bind (CESA-2021:0671)`
OID:1.3.6.1.4.1.25623.1.0.883330
Version used: `2021-08-17T06:00:55Z`

**References**
`cve: CVE-2020-8625`
`advisory-id: CESA-2021:0671`
`url: https://lists.centos.org/pipermail/centos-announce/2021-March/048281.html`
`cert-bund: CB-K21/0190`
`dfn-cert: DFN-CERT-2022-0074`
`dfn-cert: DFN-CERT-2021-0955`
`dfn-cert: DFN-CERT-2021-0556`
`dfn-cert: DFN-CERT-2021-0375`

High (CVSS: 7.5)
NVT: CentOS: Security Advisory for bind (CESA-2021:1469)

**Summary**
The remote host is missing an update for the 'bind' package(s) announced via the CESA-2021:1469 advisory.

**Vulnerability Detection Result**
`Vulnerable package: bind-export-libs`
`Installed version: bind-export-libs-9.11.4-26.P2.el7`
`Fixed version: bind-export-libs-9.11.4-26.P2.el7_9.5`

**Solution:**
**Solution type:** VendorFix
Please install the updated package(s).

**Affected Software/OS**
'bind' package(s) on CentOS 7.

**Vulnerability Insight**
The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named), a resolver library (routines for applications to use when interfacing with DNS), and tools for verifying that the DNS server is operating correctly.

... continues on next page ...

... continued from previous page ...

Security Fix(es):
bind: An assertion check can fail while answering queries for DNAME records that require the DNAME to be processed to resolve itself (CVE-2021-25215)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

**Vulnerability Detection Method**
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bind (CESA-2021:1469)`
OID:1.3.6.1.4.1.25623.1.0.883345
Version used: `2021-08-17T09:01:01Z`

**References**
`cve: CVE-2021-25215`
`advisory-id: CESA-2021:1469`
`url: https://lists.centos.org/pipermail/centos-announce/2021-April/048313.html`
`cert-bund: CB-K22/0012`
`cert-bund: CB-K21/0452`
`dfn-cert: DFN-CERT-2022-0566`
`dfn-cert: DFN-CERT-2021-1504`
`dfn-cert: DFN-CERT-2021-0915`
`dfn-cert: DFN-CERT-2021-0909`
`dfn-cert: DFN-CERT-2021-0898`

## High (CVSS: 8.3)
## NVT: CentOS: Security Advisory for binutils (CESA-2021:4033)

**Summary**
The remote host is missing an update for the 'binutils' package(s) announced via the CESA-2021:4033 advisory.

**Vulnerability Detection Result**
`Vulnerable package: binutils`
`Installed version: binutils-2.27-44.base.el7`
`Fixed version: binutils-2.27-44.base.el7_9.1`

**Solution:**
**Solution type:** VendorFix
Please install the updated package(s).

**Affected Software/OS**
'binutils' package(s) on CentOS 7.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

The binutils packages provide a collection of binary utilities for the manipulation of object code in various object file formats. It includes the ar, as, gprof, ld, nm, objcopy, objdump, ranlib, readelf, size, strings, strip, and addr2line utilities.
Security Fix(es):
Developer environment: Unicode's bidirectional (BiDi) override characters can cause trojan source attacks (CVE-2021-42574)
The following changes were introduced in binutils in order to facilitate detection of BiDi Unicode characters:
Tools which display names or strings (readelf, strings, nm, objdump) have a new command line option –unicode / -U which controls how Unicode characters are handled.
Using '–unicode=default' will treat them as normal for the tool. This is the default behaviour when –unicode option is not used. Using '–unicode=locale' will display them according to the current locale. Using '–unicode=hex' will display them as hex byte values. Using '–unicode=escape' will display them as Unicode escape sequences. Using '–unicode=highlight' will display them as Unicode escape sequences highlighted in red, if supported by the output device.
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

**Vulnerability Detection Method**
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for binutils (CESA-2021:4033)`
OID:1.3.6.1.4.1.25623.1.0.883385
Version used: `2021-11-29T14:01:10Z`

**References**
`cve: CVE-2021-42574`
`advisory-id: CESA-2021:4033`
`url: https://lists.centos.org/pipermail/centos-announce/2021-November/048395.htm`
`↪l`
`cert-bund: CB-K21/1139`
`dfn-cert: DFN-CERT-2021-2527`
`dfn-cert: DFN-CERT-2021-2275`

[ return to 10.0.28.140 ]

### 2.1.2 Medium general/tcp

Medium (CVSS: 6.5)
NVT: CentOS: Security Advisory for bind (CESA-2021:3325)

**Summary**
The remote host is missing an update for the 'bind' package(s) announced via the CESA-2021:3325 advisory.

**Vulnerability Detection Result**
`Vulnerable package: bind-export-libs`

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| Installed version: | bind-export-libs-9.11.4-26.P2.el7 |
| Fixed version: | bind-export-libs-9.11.4-26.P2.el7_9.7 |

**Solution:**
**Solution type:** VendorFix
Please install the updated package(s).

**Affected Software/OS**
'bind' package(s) on CentOS 7.

**Vulnerability Insight**
The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named), a resolver library (routines for applications to use when interfacing with DNS), and tools for verifying that the DNS server is operating correctly.
Security Fix(es):
bind: Broken inbound incremental zone update (IXFR) can cause named to terminate unexpectedly (CVE-2021-25214)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

**Vulnerability Detection Method**
Checks if a vulnerable package version is present on the target host.
Details: CentOS: Security Advisory for bind (CESA-2021:3325)
OID:1.3.6.1.4.1.25623.1.0.883376
Version used: 2021-09-03T10:01:28Z

**References**
cve: CVE-2021-25214
advisory-id: CESA-2021:3325
url: https://lists.centos.org/pipermail/centos-announce/2021-September/048361.ht
↪ml
cert-bund: CB-K21/0452
dfn-cert: DFN-CERT-2022-0566
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-2388
dfn-cert: DFN-CERT-2021-0915
dfn-cert: DFN-CERT-2021-0898

Medium (CVSS: 6.6)
NVT: CentOS: Security Advisory for bpftool (CESA-2020:5023)

**Summary**
The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2020:5023 advisory.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
Vulnerable package: kernel
Installed version:  kernel-3.10.0-1160.el7
Fixed version:      kernel-3.10.0-1160.6.1.el7
Vulnerable package: kernel-devel
Installed version:  kernel-devel-3.10.0-1160.el7
Fixed version:      kernel-devel-3.10.0-1160.6.1.el7
Vulnerable package: kernel-headers
Installed version:  kernel-headers-3.10.0-1160.el7
Fixed version:      kernel-headers-3.10.0-1160.6.1.el7
Vulnerable package: kernel-tools
Installed version:  kernel-tools-3.10.0-1160.el7
Fixed version:      kernel-tools-3.10.0-1160.6.1.el7
Vulnerable package: kernel-tools-libs
Installed version:  kernel-tools-libs-3.10.0-1160.el7
Fixed version:      kernel-tools-libs-3.10.0-1160.6.1.el7
```

**Solution:**
**Solution type:** VendorFix
Please install the updated package(s).

**Affected Software/OS**
'bpftool' package(s) on CentOS 7.

**Vulnerability Insight**
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: buffer over write in vgacon_scroll (CVE-2020-14331)
kernel: net-sysfs: *_queue_add_kobject refcount issue (CVE-2019-20811)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

... continues on next page ...

... continued from previous page ...

Bug Fix(es):OSP13, mlx5> OSP13, mlx5
SRIOV VF still sending traffic when PF is down (BZ#1733181)
gpf panic in virtio_check_driver_offered_fxature+6 when running sg_inq on a dm map for a lost virtio_blk (BZ#1811893)
GPF panic in qlt_free_session_done+626 (BZ#1826127)Brazos > Brazos
'Core(s) per socket' and 'Socket' values are interchanged in lscpu output. (kernel) (BZ#1826306)
megaraid Aero: call trace observed during reboots (BZ#1828312)
Crash in mptscsih_io_done() due to buffer overrun in sense_buf_pool (BZ#1829803)
The qedf driver fails to re-establish the online F/C port state when the downstream F/C port is toggled unless a LIP is forced (BZ#1836443)
tcp_fragment() limit causes packet drop under normal TCP load (BZ#1847765)
ip link command shows state as UNKNOWN for MACVLAN interface (BZ#1848950)
Lenovo TS 7Z60 Cooper Lake: PCI BAR firmware bug (BZ#1849223)RHEL-7/mlx4> RHEL-7/mlx4
ipoib_flush ipoib_ib_dev_flush_light [ib_ipoib] (BZ#1858707)
Uprobes crashes processes under GDB - SIGTRAP and SIGSEGV (BZ#1861396)
kernel-3.10.0-1127.19.1.el7.x86_64 crashes after an SSH connection attempt when running as a Xen PV guest on AMD Epyc Rome (BZ#1882468)
Null ptr deref after nf_reinject->nf_queue_entry_release_refs hits Attempt to release error doing inet_sock_destruct() (BZ#1885682)
Users of kernel are advised to upgrade to these updated packages, which fix these bugs.

**Vulnerability Detection Method**
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2020:5023)`
OID:1.3.6.1.4.1.25623.1.0.883300
Version used: `2021-07-06T02:00:40Z`

**References**
`cve: CVE-2019-20811`
`cve: CVE-2020-14331`
`cesa: 2020:5023`
`url: https://lists.centos.org/pipermail/centos-announce/2020-November/035868.htm`
`↪l`
`cert-bund: CB-K20/1030`
`cert-bund: CB-K20/0779`
`cert-bund: CB-K20/0523`
`dfn-cert: DFN-CERT-2022-1092`
`dfn-cert: DFN-CERT-2021-0364`
`dfn-cert: DFN-CERT-2021-0262`
`dfn-cert: DFN-CERT-2020-2588`
`dfn-cert: DFN-CERT-2020-2490`
`dfn-cert: DFN-CERT-2020-2359`
`dfn-cert: DFN-CERT-2020-2283`
`dfn-cert: DFN-CERT-2020-2229`
`dfn-cert: DFN-CERT-2020-2215`
`dfn-cert: DFN-CERT-2020-2186`
`dfn-cert: DFN-CERT-2020-2102`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2020-2064
dfn-cert: DFN-CERT-2020-2048
dfn-cert: DFN-CERT-2020-1998
dfn-cert: DFN-CERT-2020-1997
dfn-cert: DFN-CERT-2020-1987
dfn-cert: DFN-CERT-2020-1983
dfn-cert: DFN-CERT-2020-1982
dfn-cert: DFN-CERT-2020-1981
dfn-cert: DFN-CERT-2020-1972
dfn-cert: DFN-CERT-2020-1971
dfn-cert: DFN-CERT-2020-1963
dfn-cert: DFN-CERT-2020-1936
dfn-cert: DFN-CERT-2020-1935
dfn-cert: DFN-CERT-2020-1934
dfn-cert: DFN-CERT-2020-1925
dfn-cert: DFN-CERT-2020-1922
dfn-cert: DFN-CERT-2020-1912
dfn-cert: DFN-CERT-2020-1834
dfn-cert: DFN-CERT-2020-1760
dfn-cert: DFN-CERT-2020-1736
dfn-cert: DFN-CERT-2020-1709
dfn-cert: DFN-CERT-2020-1684
dfn-cert: DFN-CERT-2020-1257
```

[ return to 10.0.28.140 ]

### 2.1.3 Log general/tcp

Log (CVSS: 0.0)
NVT: Apache HTTP Server Detection Consolidation

**Summary**
Consolidation of Apache HTTP Server detections.

**Vulnerability Detection Result**

```
Detected Apache HTTP Server
Version:       2.4.6
Location:      /usr/sbin/httpd
CPE:           cpe:/a:apache:http_server:2.4.6
Concluded from version/product identification result:
Server version: Apache/2.4.6 (CentOS)
Server built:   Oct  1 2020 16:52:05
Detected Apache HTTP Server
Version:       2.4.6
Location:      443/tcp
CPE:           cpe:/a:apache:http_server:2.4.6
```

... continues on next page ...

... continued from previous page ...

```
Concluded from version/product identification result:
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_wsgi/3.4 Python/2.7.5
Detected Apache HTTP Server
Version:       2.4.6
Location:      80/tcp
CPE:           cpe:/a:apache:http_server:2.4.6
Concluded from version/product identification result:
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_wsgi/3.4 Python/2.7.5
```

**Solution:**

**Log Method**
Details: Apache HTTP Server Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.117232
Version used: 2021-02-25T13:36:35Z

**References**
url: https://httpd.apache.org

Log (CVSS: 0.0)
NVT: Authenticated Scan / LSC Info Consolidation (Linux/Unix SSH Login)

**Summary**
Consolidation and reporting of various technical information about authenticated scans / local security checks (LSC) via SSH for Linux/Unix targets.

**Vulnerability Detection Result**

```
Description (Knowledge base entry)
↪                                                : Value/Content
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-----------------------------------
Also use 'find' command to search for Applications enabled within 'Options for L
↪ocal Security Checks' (ssh/lsc/enable_find) : yes
Amount of timeouts the 'find' command has reached (ssh/lsc/find_timeout)
↪                                                : None
Clear received buffer before sending a command (ssh/force/clear_buffer)
↪                                                : FALSE
Commands are send via a pseudoterminal/pty (ssh/force/pty)
↪                                                : FALSE
Debugging enabled within 'Global variable settings' (global_settings/ssh/debug)
↪                                                : FALSE
Descend directories on other filesystem enabled within 'Options for Local Securi
↪ty Checks' (ssh/lsc/descend_ofs)                : yes
```

... continues on next page ...

... continued from previous page ...

```
Don't prepend '/bin/sh -c' to used commands (ssh/force/nosh)
↪                                                    : FALSE
Don't prepend 'LANG=C; LC_ALL=C;' to the '/bin/sh -c' commands (ssh/force/nolang
↪_sh)                                                : FALSE
Elevate Privileges Feature: Enabled
↪                                                    : FALSE
Folder exclusion regex for file search on Unixoide targets (ssh/lsc/search_exclu
↪de_paths)                                           : ^/(afs|dev|media|mnt|net|run|sfs
↪|sys|tmp|udev|var/(backups|cache|lib|local|lock|log|lost\+found|mail|opt|run|s
↪pool|tmp)|etc/init\.d|usr/share/doc)
FreeBSD package management tool available (ssh/login/freebsdpkg/available)
↪                                                    : Not applicable for target
FreeBSD patchlevel (ssh/login/freebsdpatchlevel)
↪                                                    : Not applicable for target
FreeBSD release (ssh/login/freebsdrel)
↪                                                    : Not applicable for target
Integer that sets the directory depth when using 'find' on unixoide systems (ssh
↪/lsc/find_maxdepth)                                 : 12
Login on a system with a restricted shell (ssh/restricted_shell)
↪                                                    : FALSE
Login on a system without common commands like 'cat' or 'find' (ssh/no_linux_she
↪ll)                                                 : FALSE
Login via SSH failed (login/SSH/failed)
↪                                                    : FALSE
Login via SSH successful (login/SSH/success)
↪                                                    : TRUE
Mac OS X build (ssh/login/osx_build)
↪                                                    : Not applicable for target
Mac OS X release name (ssh/login/osx_name)
↪                                                    : Not applicable for target
Mac OS X version (ssh/login/osx_version)
↪                                                    : Not applicable for target
Misconfigured CISCO device. No autocommand should be configured for the scanning
↪ user. (ssh/cisco/broken_autocommand)               : FALSE
OpenBSD version (ssh/login/openbsdversion)
↪                                                    : Not applicable for target
Operating System Key used (ssh/login/release)
↪                                                    : CentOS7
Port used for authenticated scans (kb_ssh_transport())
↪                                                    : 22/tcp
Report vulnerabilities of inactive Linux Kernel(s) separately (ssh/login/kernel_
↪reporting_overwrite/enabled)                        : FALSE
Response to 'uname -a' command (ssh/login/uname)
↪                                                    : Linux btech 3.10.0-1160.el7.x86_
↪64 #1 SMP Mon Oct 19 16:18:59 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
Send an extra command (ssh/send_extra_cmd)
↪                                                    : FALSE
```

... continues on next page ...

... continued from previous page ...

```
Solaris hardware type (ssh/login/solhardwaretype)
↪                                                : Not applicable for target
Solaris version (ssh/login/solosversion)
↪                                                : Not applicable for target
The SSH session/connection is re-opened before sending each command (ssh/force/r
↪econnect)                                       : FALSE
Use 'su - USER' option on SSH commands (ssh/lsc/use_su)
↪                                                : FALSE
Use this user for 'su - USER' option on SSH commands (ssh/lsc/su_user)
↪                                                : FALSE
User used for authenticated scans (kb_ssh_login())
↪                                                : root
locate: Command available (ssh/locate/available)
↪                                                : FALSE
locate: Response to 'locate -S' command (ssh/locate/broken)
↪                                                : /bin/sh: locate: command not fou
↪nd
rpm: Access to the RPM database failed (ssh/login/failed_rpm_db_access)
↪                                                : FALSE
NOTE: The locate command seems to be unavailable for this user/account/system. T
↪his command is highly recommended for authenticated scans to improve the searc
↪h performance on the target system. Please see the output above for a possible
↪ hint / reason why this command is not available.
```

**Solution:**

**Log Method**
Details: Authenticated Scan / LSC Info Consolidation (Linux/Unix SSH Login)
OID:1.3.6.1.4.1.25623.1.0.108162
Version used: 2021-08-02T11:07:26Z

**References**
url: https://docs.greenbone.net/GSM-Manual/gos-21.04/en/scanning.html#requiremen
↪ts-on-target-systems-with-linux-unix

## Log (CVSS: 0.0)
NVT: Authenticated Scan / LSC Info Consolidation (Linux/Unix SSH Login)

**Summary**
Consolidation and reporting of various technical information about authenticated scans / local security checks (LSC) via SSH for Linux/Unix targets.

**Vulnerability Detection Result**

```
Description (Knowledge base entry)
↪                                                : Value/Content
```

... continues on next page ...

... continued from previous page ...

```
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-----------------------------------
Also use 'find' command to search for Applications enabled within 'Options for L
↪ocal Security Checks' (ssh/lsc/enable_find) : yes
Amount of timeouts the 'find' command has reached (ssh/lsc/find_timeout)
↪                                             : None
Clear received buffer before sending a command (ssh/force/clear_buffer)
↪                                             : FALSE
Commands are send via a pseudoterminal/pty (ssh/force/pty)
↪                                             : FALSE
Debugging enabled within 'Global variable settings' (global_settings/ssh/debug)
↪                                             : FALSE
Descend directories on other filesystem enabled within 'Options for Local Securi
↪ty Checks' (ssh/lsc/descend_ofs)             : yes
Don't prepend '/bin/sh -c' to used commands (ssh/force/nosh)
↪                                             : FALSE
Don't prepend 'LANG=C; LC_ALL=C;' to the '/bin/sh -c' commands (ssh/force/nolang
↪_sh)                                         : FALSE
Elevate Privileges Feature: Enabled
↪                                             : FALSE
Folder exclusion regex for file search on Unixoide targets (ssh/lsc/search_exclu
↪de_paths)                                    : ^/(afs|dev|media|mnt|net|run|sfs
↪|sys|tmp|udev|var/(backups|cache|lib|local|lock|log|lost\+found|mail|opt|run|s
↪pool|tmp)|etc/init\.d|usr/share/doc)
FreeBSD package management tool available (ssh/login/freebsdpkg/available)
↪                                             : Not applicable for target
FreeBSD patchlevel (ssh/login/freebsdpatchlevel)
↪                                             : Not applicable for target
FreeBSD release (ssh/login/freebsdrel)
↪                                             : Not applicable for target
Integer that sets the directory depth when using 'find' on unixoide systems (ssh
↪/lsc/find_maxdepth)                          : 12
Login on a system with a restricted shell (ssh/restricted_shell)
↪                                             : FALSE
Login on a system without common commands like 'cat' or 'find' (ssh/no_linux_she
↪ll)                                          : FALSE
Login via SSH failed (login/SSH/failed)
↪                                             : FALSE
Login via SSH successful (login/SSH/success)
↪                                             : TRUE
Mac OS X build (ssh/login/osx_build)
↪                                             : Not applicable for target
Mac OS X release name (ssh/login/osx_name)
↪                                             : Not applicable for target
Mac OS X version (ssh/login/osx_version)
```

... continues on next page ...

... continued from previous page ...

```
↪                                                    : Not applicable for target
Misconfigured CISCO device. No autocommand should be configured for the scanning
↪ user. (ssh/cisco/broken_autocommand)               : FALSE
OpenBSD version (ssh/login/openbsdversion)
↪                                                    : Not applicable for target
Operating System Key used (ssh/login/release)
↪                                                    : CentOS7
Port used for authenticated scans (kb_ssh_transport())
↪                                                    : 22/tcp
Report vulnerabilities of inactive Linux Kernel(s) separately (ssh/login/kernel_
↪reporting_overwrite/enabled)                        : FALSE
Response to 'uname -a' command (ssh/login/uname)
↪                                                    : Linux btech 3.10.0-1160.el7.x86_
↪64 #1 SMP Mon Oct 19 16:18:59 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
Send an extra command (ssh/send_extra_cmd)
↪                                                    : FALSE
Solaris hardware type (ssh/login/solhardwaretype)
↪                                                    : Not applicable for target
Solaris version (ssh/login/solosversion)
↪                                                    : Not applicable for target
The SSH session/connection is re-opened before sending each command (ssh/force/r
↪econnect)                                           : FALSE
Use 'su - USER' option on SSH commands (ssh/lsc/use_su)
↪                                                    : FALSE
Use this user for 'su - USER' option on SSH commands (ssh/lsc/su_user)
↪                                                    : FALSE
User used for authenticated scans (kb_ssh_login())
↪                                                    : root
locate: Command available (ssh/locate/available)
↪                                                    : FALSE
locate: Response to 'locate -S' command (ssh/locate/broken)
↪                                                    : /bin/sh: locate: command not fou
↪nd
rpm: Access to the RPM database failed (ssh/login/failed_rpm_db_access)
↪                                                    : FALSE
NOTE: The locate command seems to be unavailable for this user/account/system. T
↪his command is highly recommended for authenticated scans to improve the searc
↪h performance on the target system. Please see the output above for a possible
↪ hint / reason why this command is not available.
```

**Solution:**

**Log Method**

Details: Authenticated Scan / LSC Info Consolidation (Linux/Unix SSH Login)
OID:1.3.6.1.4.1.25623.1.0.108162
Version used: 2021-08-02T11:07:26Z

... continues on next page ...

... continued from previous page ...

**References**
url: https://docs.greenbone.net/GSM-Manual/gos-21.04/en/scanning.html#requiremen
↪ts-on-target-systems-with-linux-unix

Log (CVSS: 0.0)
NVT: BIOS and Hardware Information Detection (Linux/Unix SSH Login)

**Summary**
SSH login-based gathering of various BIOS and Hardware related information.

**Vulnerability Detection Result**
BIOS version: 6.00
BIOS Vendor: Phoenix Technologies LTD
Base Board version: None
Base Board Manufacturer: Intel Corporation
Base Board Product Name: 440BX Desktop Reference Platform

**Solution:**

**Log Method**
Logs in via SSH and queries the BIOS and Hardware related information using the command line tool 'dmidecode'. Usually this command requires root privileges to execute.
Details: BIOS and Hardware Information Detection (Linux/Unix SSH Login)
OID:1.3.6.1.4.1.25623.1.0.800163
Version used: 2021-06-07T11:59:32Z

[ return to 10.0.28.140 ]