Scan Report

December 9, 2018

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "UTC", which is abbreviated "UTC". The task was "rz.lab - internal network assessment". The scan started at Sun Dec 9 15:22:26 2018 UTC and ended at Sun Dec 9 16:10:43 2018 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
10.100.10.1 router.rz.lab	0	2	2	0	1
10.100.10.11 docker-manager.rz.lab	0	0	3	0	1
10.100.10.12 docker-worker.rz.lab	0	0	3	0	1
10.100.10.3 utility.rz.lab	0	0	3	0	1
10.100.10.2 acs.rz.lab	0	0	2	0	1
10.100.10.4 dc.rz.lab	0	0	2	0	1
Total: 6	0	2	15	0	6

Vendor security updates are trusted, using full CVE matching.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.
It only lists hosts that produced issues.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.

This report contains all 23 results selected by the filtering described above. Before filtering there were 203 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.100.10.1 - router.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant
10.100.10.11 - docker-manager.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant
10.100.10.12 - docker-worker.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant
10.100.10.3 - utility.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant
10.100.10.2 - acs.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant
10.100.10.4 - dc.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant

2 Results per Host

2.1 10.100.10.1

Host scan start Sun Dec 9 15:22:43 2018 UTC
Host scan end Sun Dec 9 16:00:13 2018 UTC

Service (Port)	Threat Level
53/tcp	Medium
22/tcp	Low
general/tcp	False Positive

2.1.1 Medium 53/tcp

Medium (Overridden from High)
NVT: ISC BIND 'deny-answer-aliases' Denial of Service Vulnerability

Product detection result
`cpe:/a:isc:bind:9.11.3.1ubuntu1.3`
`Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1`
`↪.4.1.25623.1.0.10028)`

Summary
The host is installed with ISC BIND and is prone to a denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 9.11.3.1ubuntu1.3`
`Fixed version: 9.11.4-P1`

Impact
Successful exploitation will allow remote attackers to cause a denial of service (assertion failure).

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.13-P1 or 9.10.8-P1 or 9.11.4-P1 or 9.12.2-P1 or 9.11.3-S3 or later. For updates refer to Reference links.

Affected Software/OS
ISC BIND versions 9.7.0 through 9.8.8, 9.9.0 through 9.9.13, 9.10.0 through 9.10.8, 9.11.0 through 9.11.4, 9.12.0 through 9.12.2 and 9.13.0 through 9.13.2.

Vulnerability Insight
The flaw exists due to a defect in the feature 'deny-answer-aliases' which leads to assertion failure in 'name.c'.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: ISC BIND 'deny-answer-aliases' Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.813750
Version used: $Revision: 12116 $

Product Detection Result
Product: cpe:/a:isc:bind:9.11.3.1ubuntu1.3
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2018-5740
Other:
URL:https://kb.isc.org/article/AA-01639/0
URL:https://kb.isc.org/article/AA-01646/81/BIND-9.11.3-S3-Release-Notes.html
URL:https://kb.isc.org/article/AA-01645/81/BIND-9.12.2-P1-Release-Notes.html
URL:https://kb.isc.org/article/AA-01644/81/BIND-9.11.4-P1-Release-Notes.html
URL:https://kb.isc.org/article/AA-01643/81/BIND-9.10.8-P1-Release-Notes.html
URL:https://kb.isc.org/article/AA-01642/81/BIND-9.9.13-P1-Release-Notes.html
URL:https://www.isc.org

Medium (CVSS: 4.3)
NVT: ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability

Product detection result
cpe:/a:isc:bind:9.11.3.1ubuntu1.3
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
ISC BIND is prone to a remote denial-of-service vulnerability because the application fails to properly handle specially crafted dynamic update requests.

Vulnerability Detection Result
It seems that OpenVAS was able to crash the remote Bind.
Please check its status right now.

Impact
Successfully exploiting this issue allows remote attackers to crash affected DNS servers, denying further service to legitimate users.

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

The vendor released an advisory and fixes to address this issue. Please see the references for more information.

Affected Software/OS
Versions prior to BIND 9.4.3-P3, 9.5.1-P3, and 9.6.1-P1 are vulnerable.

Vulnerability Detection Method
Details: `ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100251
Version used: `$Revision: 4436 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.11.3.1ubuntu1.3`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
```
CVE: CVE-2009-0696
BID:35848
Other:
  URL:http://www.securityfocus.com/bid/35848
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=514292
   URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=538975
   URL:http://www.isc.org/products/BIND/
   URL:https://www.isc.org/node/474
   URL:http://www.kb.cert.org/vuls/id/725188
```

[return to 10.100.10.1]

2.1.2 Low 22/tcp

Low (Overridden from Medium)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

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

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
```

... continues on next page ...

... continued from previous page ...

```
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: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

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: `$Revision: 12116 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2018-15473`
`Other:`
`URL:http://www.openssh.com`
`URL:https://0day.city/cve-2018-15473.html`
`URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a`
`↪7d1e0`

Low (Overridden from Medium)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

... continues on next page ...

... continued from previous page ...

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

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

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

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

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: `$Revision: 12308 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2018-15919
Other:
  URL:http://www.openssh.com
   URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
   URL:https://seclists.org/oss-sec/2018/q3/180
```

[return to 10.100.10.1]

2.1.3 False Positive general/tcp

False Positive (Overridden from Medium) NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)
Summary This host is installed with GZip and is prone to Input Validation Vulnerability
Vulnerability Detection Result `The target host was found to be vulnerable`
Impact Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.
Solution **Solution type:** VendorFix Update to GZip version 1.3.13 or later.
Affected Software/OS GZip version prior to 1.3.13 on Linux.
Vulnerability Insight The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.
Vulnerability Detection Method Details: `GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)` OID:1.3.6.1.4.1.25623.1.0.800453 Version used: `$Revision: 12690 $`

References
`CVE: CVE-2009-2624`
`BID:37888`
`Other:`
`URL:http://secunia.com/advisories/38132`
`URL:http://www.vupen.com/english/advisories/2010/0185`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711`
`URL:http://www.gzip.org/index-f.html#sources`
`URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338`
`↪1dba5032f4dfc1744cf2`

[return to 10.100.10.1]

2.2 10.100.10.11

Host scan start	Sun Dec 9 15:22:43 2018 UTC
Host scan end	Sun Dec 9 16:05:53 2018 UTC

Service (Port)	Threat Level
22/tcp	Low
general/tcp	Low
general/tcp	False Positive

2.2.1 Low 22/tcp

Low (Overridden from Medium)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

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

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
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: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

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

. . . continues on next page . . .

... continued from previous page ...

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: $Revision: 12116 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2018-15473
Other:
URL:http://www.openssh.com
URL:https://0day.city/cve-2018-15473.html
URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0

Low (Overridden from Medium)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

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

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

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

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

OpenSSH version 5.9 to 7.8 on Linux.

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: `$Revision: 12308 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2018-15919
Other:
  URL:http://www.openssh.com
   URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
   URL:https://seclists.org/oss-sec/2018/q3/180
```

[return to 10.100.10.11]

2.2.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 4152699885
Packet 2: 4152700938
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 10411 $`

References
`Other:`
`URL:http://www.ietf.org/rfc/rfc1323.txt`

Note

```
vagrant@docker-manager:~$ sudo ./verify_tcp_timestamps_mitigation.sh
tcp_timestamps Status for Container Host:
net.ipv4.tcp_timestamps = 0
/usr/bin/docker
CONTAINER ID        IMAGE               COMMAND                  CREATED
↪     STATUS              PORTS               NAMES
618c683b4e9c        traefik:1.7.5       "/traefik --debug=tr..."   2 days ago
↪     Up 2 days           80/tcp              lbr_traefik.lr51y1kymw9ojw8pheyi2
↪b168.xb97dmsh4wmklhjl74ropby1y
tcp_timestamps Status for guest containers:
618c683b4e9c: OCI runtime exec failed: exec failed: container_linux.go:348: star
↪ting container process caused "exec: \"sysctl\": executable file not found in
↪$PATH": unknown
Container host confirmed to have mitigated this vulnerability detection result.
traefik container image assumed to be implementing RFC 1323.
sysctl binary was not available on traefik container image to verify mitigation
↪status.
```

... continues on next page ...

. . . continued from previous page . . .

Last modified: Sun Dec 9 16:19:19 2018 UTC

[return to 10.100.10.11]

2.2.3 False Positive general/tcp

False Positive (Overridden from Medium)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: `GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: `$Revision: 12690 $`

References
`CVE: CVE-2009-2624`
`BID:37888`
`Other:`
`URL:http://secunia.com/advisories/38132`
`URL:http://www.vupen.com/english/advisories/2010/0185`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711`
`URL:http://www.gzip.org/index-f.html#sources`
`URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338`
`↪1dba5032f4dfc1744cf2`

[return to 10.100.10.11]

2.3 10.100.10.12

Host scan start Sun Dec 9 15:22:43 2018 UTC
Host scan end Sun Dec 9 16:05:53 2018 UTC

Service (Port)	Threat Level
general/tcp	Low
22/tcp	Low
general/tcp	False Positive

2.3.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1249564279
Packet 2: 1249565289
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: TCP timestamps
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: $Revision: 10411 $

References
Other:
URL:http://www.ietf.org/rfc/rfc1323.txt

Note

```
vagrant@docker-worker:~$ sudo ./verify_tcp_timestamps_mitigation.sh
tcp_timestamps Status for Container Host:
net.ipv4.tcp_timestamps = 0
/usr/bin/docker
CONTAINER ID        IMAGE               COMMAND                  CREATED
↪     STATUS              PORTS                 NAMES
960cb9d24d3f        wordpress:latest    "docker-entrypoint.s..."   35 hours ago
↪     Up 35 hours         80/tcp                blog_wordpress.1.don6vicmultaxt
↪3t4pquj7hdt
76d977508cff        mysql:5.7           "docker-entrypoint.s..."   2 days ago
↪     Up 2 days           3306/tcp, 33060/tcp   blog_db.1.y83cylgdl7jrwjz5hzdvl
↪uxxo
tcp_timestamps Status for guest containers:
960cb9d24d3f: net.ipv4.tcp_timestamps = 1
76d977508cff: OCI runtime exec failed: exec failed: container_linux.go:348: star
↪ting container process caused "exec: \"sysctl\": executable file not found in
↪$PATH": unknown
Container host confirmed to have mitigated this vulnerability detection result.
wordpress container image confirmed to be implementing RFC 1323.
mysql container image assumed to be implementing RFC 1323.
sysctl binary was not available on the mysql container image to verify mitigatio
↪n status.
```

Last modified: Sun Dec 9 16:18:32 2018 UTC

[return to 10.100.10.12]

2.3.2 Low 22/tcp

Low (Overridden from Medium)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

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

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: NoneAvailable
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: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

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: $Revision: 12116 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2018-15473
Other:
URL:http://www.openssh.com

... continues on next page ...

... continued from previous page ...

URL:https://0day.city/cve-2018-15473.html
URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0

Low (Overridden from Medium)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

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

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

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

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

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: $Revision: 12308 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1

... continues on next page ...

... continued from previous page ...

Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2018-15919
Other:
URL:http://www.openssh.com
URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
URL:https://seclists.org/oss-sec/2018/q3/180

[return to 10.100.10.12]

2.3.3 False Positive general/tcp

False Positive (Overridden from Medium)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: $Revision: 12690 $

References
CVE: CVE-2009-2624

... continues on next page ...

... continued from previous page ...

```
BID:37888
Other:
  URL:http://secunia.com/advisories/38132
   URL:http://www.vupen.com/english/advisories/2010/0185
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
   URL:http://www.gzip.org/index-f.html#sources
   URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338
↪1dba5032f4dfc1744cf2
```

[return to 10.100.10.12]

2.4 10.100.10.3

Host scan start	Sun Dec 9 15:22:43 2018 UTC
Host scan end	Sun Dec 9 16:10:40 2018 UTC

Service (Port)	Threat Level
22/tcp	Low
general/tcp	Low
general/tcp	False Positive

2.4.1 Low 22/tcp

Low (Overridden from Medium)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
```

Summary

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

Vulnerability Detection Result

```
Installed version: 7.6p1
Fixed version:     NoneAvailable
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

... continues on next page ...

... continued from previous page ...

Solution type: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

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: `$Revision: 12116 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2018-15473
Other:
  URL:http://www.openssh.com
   URL:https://0day.city/cve-2018-15473.html
   URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0
```

Low (Overridden from Medium)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
```
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
```

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

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
Installation
```

... continues on next page ...

... continued from previous page ...

path / port: 22/tcp

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

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

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: $Revision: 12308 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2018-15919
Other:
URL:http://www.openssh.com
URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
URL:https://seclists.org/oss-sec/2018/q3/180

[return to 10.100.10.3]

2.4.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

... continues on next page ...

... continued from previous page ...

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1240493766
Packet 2: 1240494778
```

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS

TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: `TCP timestamps`

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: `$Revision: 10411 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

Note

```
vagrant@utility:~$ sudo ./verify_tcp_timestamps_mitigation.sh
tcp_timestamps Status for Container Host:
net.ipv4.tcp_timestamps = 0
/usr/bin/docker
CONTAINER ID        IMAGE                                                CO
```

... continues on next page ...

... continued from previous page ...

```
↪MMAND                  CREATED             STATUS              PORTS
↪      NAMES
b0a03ad874e7        docker.elastic.co/logstash/logstash-oss:6.5.0             "/
↪usr/local/bin/dock..."   3 days ago          Up 3 days           5044/tcp, 9600/
↪tcp   elk_logstash.1.zsdd592xd2tz8z94j5y5blf2w
514bf68d6ad3        docker.elastic.co/elasticsearch/elasticsearch-oss:6.5.0   "/
↪usr/local/bin/dock..."   3 days ago          Up 3 days           9200/tcp, 9300/
↪tcp   elk_elasticsearch.1.jbtbx5yenu3bu1j3bkwncbymq
ec510d73f649        docker.elastic.co/kibana/kibana-oss:6.5.0                 "/
↪usr/local/bin/kiba..."   3 days ago          Up 3 days           5601/tcp
↪      elk_kibana.1.tpo6edfno68tk3lkycac6ipax
tcp_timestamps Status for guest containers:
b0a03ad874e7: net.ipv4.tcp_timestamps = 1
514bf68d6ad3: net.ipv4.tcp_timestamps = 1
ec510d73f649: net.ipv4.tcp_timestamps = 1
Container host confirmed to have mitigated this vulnerability detection result.
elasticsearch container image confirmed to be implementing RFC 1323
kibana container image confirmed to be implementing RFC 1323
logstash container image confirmed to be implementing RFC 1323
```

Last modified: Sun Dec 9 16:17:04 2018 UTC

[return to 10.100.10.3]

2.4.3 False Positive general/tcp

False Positive (Overridden from Medium)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: $Revision: 12690 $

References
CVE: CVE-2009-2624
BID:37888
Other:
URL:http://secunia.com/advisories/38132
URL:http://www.vupen.com/english/advisories/2010/0185
URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
URL:http://www.gzip.org/index-f.html#sources
URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338
↪1dba5032f4dfc1744cf2

[return to 10.100.10.3]

2.5 10.100.10.2

Host scan start Sun Dec 9 15:22:43 2018 UTC
Host scan end Sun Dec 9 15:56:45 2018 UTC

Service (Port)	Threat Level
22/tcp	Low
general/tcp	False Positive

2.5.1 Low 22/tcp

Low (Overridden from Medium)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Installed version: 7.6p1
Fixed version:     NoneAvailable
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: NoneAvailable

No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

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: `$Revision: 12116 $`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:7.6p1`

Method: `SSH Server type and version`

OID: 1.3.6.1.4.1.25623.1.0.10267)

References

```
CVE: CVE-2018-15473
Other:
  URL:http://www.openssh.com
   URL:https://0day.city/cve-2018-15473.html
   URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0
```

Low (Overridden from Medium)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

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

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

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

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

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: $Revision: 12308 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2018-15919
Other:
URL:http://www.openssh.com
URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163

... continues on next page ...

... continued from previous page ...

URL:https://seclists.org/oss-sec/2018/q3/180

[return to 10.100.10.2]

2.5.2 False Positive general/tcp

False Positive (Overridden from Medium)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: $Revision: 12690 $

References
CVE: CVE-2009-2624
BID:37888
Other:
URL:http://secunia.com/advisories/38132
URL:http://www.vupen.com/english/advisories/2010/0185
URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
URL:http://www.gzip.org/index-f.html#sources
URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338
↪1dba5032f4dfc1744cf2

[return to 10.100.10.2]

2.6 10.100.10.4

Host scan start Sun Dec 9 15:22:43 2018 UTC
Host scan end Sun Dec 9 16:02:51 2018 UTC

Service (Port)	Threat Level
22/tcp	Low
general/tcp	False Positive

2.6.1 Low 22/tcp

Low (Overridden from Medium)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

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

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
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: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

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

. . . continues on next page . . .

... continued from previous page ...

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: `$Revision: 12116 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2018-15473
Other:
  URL:http://www.openssh.com
   URL:https://0day.city/cve-2018-15473.html
   URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0
```

Low (Overridden from Medium)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
```
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
```

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

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

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

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

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: `$Revision: 12308 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2018-15919`
`Other:`
`URL:http://www.openssh.com`
`URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163`
`URL:https://seclists.org/oss-sec/2018/q3/180`

[return to 10.100.10.4]

2.6.2 False Positive general/tcp

False Positive (Overridden from Medium)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: $Revision: 12690 $

References
CVE: CVE-2009-2624
BID:37888
Other:
URL:http://secunia.com/advisories/38132
URL:http://www.vupen.com/english/advisories/2010/0185
URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
URL:http://www.gzip.org/index-f.html#sources
URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338
↪1dba5032f4dfc1744cf2

[return to 10.100.10.4]