Scan Report

November 2, 2023

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 “scan1”. The scan started at Thu Nov 2 21:40:04 2023 UTC and ended at Thu Nov 2 21:49:32 2023 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
10.200.0.11 ns1.seclab.net	16	22	6	11	0
Total: 1	16	22	6	11	0

Vendor security updates are not trusted.
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.

This report contains all 55 results selected by the filtering described above. Before filtering there were 55 results.

2 Results per Host

2.1 10.200.0.11

Host scan start	Thu Nov 2 21:40:21 2023 UTC
Host scan end	Thu Nov 2 21:49:32 2023 UTC

Service (Port)	Threat Level
22/tcp	High
53/tcp	High
22/tcp	Medium
general/tcp	Medium
53/tcp	Medium
22/tcp	Low
general/tcp	Low
53/tcp	Low
22/tcp	Log
general/tcp	Log
general/icmp	Log
general/CPE-T	Log
53/tcp	Log

2.1.1 High 22/tcp

High (CVSS: 7.5)
NVT: OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:openbsd:openssh:5.3
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

OpenSSH is prone to a remote memory-corruption vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     See references
Installation
path / port:       22/tcp
```

Impact

An attacker can exploit this issue to execute arbitrary code in context of the application. Failed exploits may result in denial-of-service conditions.

Solution

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

OpenSSH 6.4 and prior with J-PAKE implemented are vulnerable.

Vulnerability Insight

The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.105001

Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2014-1692
BID:65230
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

URL:http://www.securityfocus.com/bid/65230

High (CVSS: 7.8)
NVT: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:5.3
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 denial of service and user enumeration vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     7.3
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided.

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.3 or later.

Affected Software/OS

OpenSSH versions before 7.3 on Linux

Vulnerability Insight

Multiple flaws exist due to,

- The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication.

- The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)`

OID:1.3.6.1.4.1.25623.1.0.809154

Version used: `2019-05-21T12:48:06+0000`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-6515, CVE-2016-6210
BID:92212
Other:
  URL:http://www.openssh.com/txt/release-7.3
   URL:http://seclists.org/fulldisclosure/2016/Jul/51
   URL:https://security-tracker.debian.org/tracker/CVE-2016-6210
   URL:http://openwall.com/lists/oss-security/2016/08/01/2
```

High (CVSS: 8.5)
NVT: OpenSSH Multiple Vulnerabilities

Product detection result

```
cpe:/a:openbsd:openssh:5.3
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

This host is running OpenSSH and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     7.0
Installation
path / port:       22/tcp
```

Impact

Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service.

Solution

Solution type: VendorFix
Upgrade to OpenSSH 7.0 or later.

Affected Software/OS

OpenSSH versions before 7.0.

Vulnerability Insight

Multiple flaws are due to:
- Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd.
- Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd.

. . . continues on next page . . .

. . . continued from previous page . . .

- Vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `OpenSSH Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.806052
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2015-6564, CVE-2015-6563, CVE-2015-5600
Other:
  URL:http://seclists.org/fulldisclosure/2015/Aug/54
   URL:http://openwall.com/lists/oss-security/2015/07/23/4
```

High (CVSS: 7.5)
NVT: OpenSSH Multiple Vulnerabilities Jan17 (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:5.3
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 multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     7.4
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules.

Solution

Solution type: VendorFix
Upgrade to OpenSSH version 7.4 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
OpenSSH versions before 7.4 on Linux

Vulnerability Insight
Multiple flaws exists due to,
- An 'authfile.c' script does not properly consider the effects of realloc on buffer contents.
- The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers.
- The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used.
- An untrusted search path vulnerability in ssh-agent.c in ssh-agent.
- NULL pointer dereference error due to an out-of-sequence NEWKEYS message.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH Multiple Vulnerabilities Jan17 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.8103256
Version used: `2019-05-21T12:48:06+0000`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10
↪708
BID:94968, 94972, 94977, 94975
Other:
  URL:https://www.openssh.com/txt/release-7.4
   URL:http://www.openwall.com/lists/oss-security/2016/12/19/2
   URL:http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html
   URL:https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e
↪933e6b931de1d16737
```

High (CVSS: 7.2)
NVT: OpenSSH Privilege Escalation Vulnerability - May16

Product detection result

```
cpe:/a:openbsd:openssh:5.3
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 privilege escalation vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     7.2p2-3
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue will allow local users to gain privileges.

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.2p2-3 or later.

Affected Software/OS

OpenSSH versions through 7.2p2.

Vulnerability Insight

The flaw exists due to an error in 'do_setup_env function' in 'session.c' script in sshd which trigger a crafted environment for the /bin/login program when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: OpenSSH Privilege Escalation Vulnerability - May16

OID:1.3.6.1.4.1.25623.1.0.807574

Version used: 2019-05-22T07:58:25+0000

Product Detection Result

Product: cpe:/a:openbsd:openssh:5.3

Method: OpenSSH Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2015-8325
Other:
  URL:https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html
   URL:https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4
↪e10a65c91810f88755
```

High (CVSS: 7.5)

NVT: OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:5.3
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
This host is installed with openssh and is prone to security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     7.2
Installation
path / port:       22/tcp
```

Impact
Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.2 or later.

Affected Software/OS
OpenSSH versions before 7.2 on Linux.

Vulnerability Insight
An access flaw was discovered in OpenSSH, It did not correctly handle failures to generate authentication cookies for untrusted X11 forwarding. A malicious or compromised remote X application could possibly use this flaw to establish a trusted connection to the local X server, even if only untrusted X11 forwarding was requested.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.810769
Version used: `2019-05-22T12:00:57+0000`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-1908
BID:84427
Other:
  URL:http://openwall.com/lists/oss-security/2016/01/15/13
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4
   URL:http://www.openssh.com/txt/release-7.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
   URL:https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6f
↪a0db113c71e234416c
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741
```

High (CVSS: 7.5)
NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.
As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

```
It was possible to login with the following credentials <User>:<Password>
root:password
```

Solution
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Try to login with a number of known default credentials via the SSH protocol.
Details: `SSH Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: `$Revision: 13568 $`

[return to 10.200.0.11]

2.1.2 High 53/tcp

High (CVSS: 10.0)
NVT: BIND End of Life Detection (Linux)

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)
```

Summary
The BIND version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
The "BIND" version on the remote host has reached the end of life.
CPE:               cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
EOL version:       9.8
EOL date:          2014-09-30
```

Impact

An end of life version of BIND is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

Solution type: VendorFix

Update the BIND version on the remote host to a still supported version.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `BIND End of Life Detection (Linux)`

OID:1.3.6.1.4.1.25623.1.0.113016

Version used: `$Revision: 11935 $`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`

Method: `Determine which version of BIND name daemon is running`

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
Other:
  URL:https://www.isc.org/downloads/software-support-policy/
   URL:https://www.isc.org/downloads/
```

High (CVSS: 7.8)

NVT: ISC BIND 'buffer.c' Assertion Failure Denial of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.9-P3
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.9-P3 or 9.10.4-P3 or 9.11.0rc3 or later on Linux.

Affected Software/OS
ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 on Linux.

Vulnerability Insight
The flaw exists due to the 'buffer.c' script in named in ISC BIND does not properly construct responses.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ISC BIND 'buffer.c' Assertion Failure Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.810263
Version used: `2019-07-05T09:54:18+0000`

Product Detection Result
Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2016-2776
BID:93188
Other:
  URL:https://kb.isc.org/article/AA-01419/0
```

High (CVSS: 7.8)
NVT: ISC BIND 'buffer.c' Script Remote Denial of Service Vulnerability - Jan16

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 remote denial of service vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.7-P3
```

Impact

Successful exploitation will allow remote attackers to cause denial of service.

Solution

Solution type: VendorFix

Upgrade to ISC BIND version 9.9.7-P3 or 9.10.2-P4 or later.

Affected Software/OS

ISC BIND versions 9.0.0 through 9.8.8 and 9.9.0 through 9.9.7-P2 and 9.10.x through 9.10.2-P3.

Vulnerability Insight

The flaw is due to an error in 'buffer.c' script in ISC BIND.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `ISC BIND 'buffer.c' Script Remote Denial of Service Vulnerability - Jan16`

OID:1.3.6.1.4.1.25623.1.0.807202

Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`

Method: `Determine which version of BIND name daemon is running`

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2015-5722
BID:76605
Other:
  URL:https://kb.isc.org/article/AA-01287
```

High (CVSS: 7.8)

NVT: ISC BIND Delegation Handling Denial of Service Vulnerability

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 denial of service vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     Upgrade to 9.9.6-P1
```

Impact

Successful exploitation will allow attackers to cause denial of service to clients.

Solution

Solution type: VendorFix

Upgrade to ISC BIND version 9.9.6-p1 or 9.10.1-p1 or later for branches of BIND (9.9 and 9.10).

Affected Software/OS

ISC BIND versions 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1

Vulnerability Insight

The flaw is due to ISC BIND does not handle delegation chaining properly.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `ISC BIND Delegation Handling Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.806080
Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2014-8500
Other:
  URL:https://kb.isc.org/article/AA-01216/0/
```

High (CVSS: 7.8)
NVT: ISC BIND Denial of Service Vulnerability

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 denial of service vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.9-P3
```

Impact

An remote attacker may cause a denial of service condition.

Solution

Solution type: VendorFix

Upgrade to 9.9.9-P3, 9.9.9-S5, 9.10.4-P3, 9.11.0rc3 or later.

Affected Software/OS

BIND 9

Vulnerability Insight

A crafted query could crash the BIND name server daemon, leading to a denial of service. All server roles (authoritative, recursive and forwarding) in default configurations are affected.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `ISC BIND Denial of Service Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.106291

Version used: `2019-07-24T08:39:52+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`

Method: `Determine which version of BIND name daemon is running`

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2016-2776
Other:
  URL:https://kb.isc.org/article/AA-01419
```

High (CVSS: 7.8)

NVT: ISC BIND Denial of Service Vulnerability - 06 - Jan16

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.7-P2
```

Impact

Successful exploitation will allow remote attackers to cause denial of service.

Solution

Solution type: VendorFix

Upgrade to ISC BIND version 9.9.7-P2 or 9.10.2-P3 or later.

Affected Software/OS

ISC BIND versions 9.1.0 through 9.9.7-P1, 9.10.0 through 9.10.2-P2.

Vulnerability Insight

The flaw is due to an error in handling TKEY queries can cause named to exit with a REQUIRE assertion failure.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `ISC BIND Denial of Service Vulnerability - 06 - Jan16`

OID:1.3.6.1.4.1.25623.1.0.807200

Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`

Method: `Determine which version of BIND name daemon is running`

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2015-5477
BID:76092
Other:
  URL:https://kb.isc.org/article/AA-01272
```

High (CVSS: 7.8)

NVT: ISC BIND Denial of Service Vulnerability - Oct15

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

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

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.7-P1
```

Impact

Successful exploitation will allow attackers to cause denial of service to clients.

Solution

Solution type: VendorFix

Upgrade to ISC BIND version 9.9.7-P1 or 9.10.2-P2 or later.

Affected Software/OS

ISC BIND versions 9.7.x through 9.9.x before 9.9.7-P1 and 9.10.x before 9.10.2-P2

Vulnerability Insight

The flaw is due to an error in 'name.c' script in ISC BIND when configured as a recursive resolver with DNSSEC validation.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `ISC BIND Denial of Service Vulnerability - Oct15`

OID:1.3.6.1.4.1.25623.1.0.806079

Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`

Method: `Determine which version of BIND name daemon is running`

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2015-4620
Other:
  URL:https://kb.isc.org/article/AA-01267
```

High (CVSS: 7.8)

NVT: ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability - Jan16

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

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

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.8.3-P4
```

Impact

Successful exploitation will allow attackers to cause denial of service.

Solution

Solution type: VendorFix

Upgrade to ISC BIND version 9.7.7 or 9.7.6-P4 or 9.6-ESV-R8 or 9.6-ESV-R7-P4 or 9.8.4 or 9.8.3-P4 or 9.9.2 or 9.9.1-P4 later.

Affected Software/OS

ISC BIND versions 9.2.x through 9.6.x, 9.4-ESV through 9.4-ESV-R5-P1, 9.6-ESV through 9.6-ESV-R7-P3, 9.7.0 through 9.7.6-P3, 9.8.0 through 9.8.3-P3, 9.9.0 through 9.9.1-P3.

Vulnerability Insight

The flaw exists due to an error in DNS RDATA Handling in ISC BIND.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability - Jan16`

OID:1.3.6.1.4.1.25623.1.0.807203

Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`

Method: `Determine which version of BIND name daemon is running`

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2012-5166
BID:55852
Other:
  URL:https://kb.isc.org/article/AA-00801
```

High (CVSS: 7.8)

NVT: ISC BIND DNS64 Remote Denial of Service Vulnerability - Jan16

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 remote denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.8.4-P1
```

Impact
Successful exploitation will allow remote attackers to cause denial of service.

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.8.4-P1 or 9.9.2-P1 or later.

Affected Software/OS
ISC BIND versions 9.8.x before 9.8.4-P1 and 9.9.x before 9.9.2-P1.

Vulnerability Insight
The flaw exists due to some unspecified error in ISC BIND when DNS64 is enabled.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ISC BIND DNS64 Remote Denial of Service Vulnerability - Jan16`
OID:1.3.6.1.4.1.25623.1.0.807204
Version used: `2019-07-05T09:54:18+0000`

Product Detection Result
Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2012-5688
BID:56817
Other:
  URL:https://kb.isc.org/article/AA-00828
```

[return to 10.200.0.11]

2.1.3 Medium 22/tcp

Medium (CVSS: 5.8)
NVT: OpenSSH 'child_set_env()' Function Security Bypass Vulnerability

Product detection result

```
cpe:/a:openbsd:openssh:5.3
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

OpenSSH is prone to a security-bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     6.6
Installation
path / port:       22/tcp
```

Impact

The security bypass allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.

Solution

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Versions prior to OpenSSH 6.6 are vulnerable.

Vulnerability Insight

sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'child_set_env()' Function Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105003
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2014-2532
BID:66355
Other:
```

... continues on next page ...

. . . continued from previous page . . .

```
URL:http://www.securityfocus.com/bid/66355
```

Medium (CVSS: 5.0)
NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:5.3
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 security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     7.6
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.6 or later.

Affected Software/OS

OpenSSH versions before 7.6 on Linux

Vulnerability Insight

The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.812051
Version used: `2019-05-23T14:08:05+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2017-15906
BID:101552
Other:
  URL:https://www.openssh.com/txt/release-7.6
   URL:https://github.com/openbsd/src/commit/a6981567e8e
```

Medium (CVSS: 5.5)
NVT: OpenSSH <= 7.2p1 - Xauth Injection

Product detection result

```
cpe:/a:openbsd:openssh:5.3
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

openssh xauth command injection may lead to forced-command and /bin/false bypass

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     7.2p2
Installation
path / port:       22/tcp
```

Impact

By injecting xauth commands one gains limited* read/write arbitrary files, information leakage or xauth-connect capabilities.

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.2p2 or later.

Affected Software/OS

OpenSSH versions before 7.2p2.

Vulnerability Insight

An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie. The newline acts as a command separator to the xauth binary. This attack requires the server to have 'X11Forwarding yes' enabled. Disabling it, mitigates this vector.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `OpenSSH <= 7.2p1 - Xauth Injection`

OID:1.3.6.1.4.1.25623.1.0.105581

Version used: `2019-05-22T07:58:25+0000`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-3115
Other:
  URL:http://www.openssh.com/txt/release-7.2p2
```

Medium (CVSS: 5.8)
NVT: OpenSSH Certificate Validation Security Bypass Vulnerability

Product detection result

```
cpe:/a:openbsd:openssh:5.3
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary
OpenSSH is prone to a security-bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     See references
Installation
path / port:       22/tcp
```

Impact
Attackers can exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
OpenSSH 6.6 and prior are vulnerable.

Vulnerability Insight
The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `OpenSSH Certificate Validation Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105004
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2014-2653
BID:66459
Other:
  URL:http://www.securityfocus.com/bid/66459
```

Medium (CVSS: 5.0)
NVT: OpenSSH Denial of Service Vulnerability

Product detection result

```
cpe:/a:openbsd:openssh:5.3
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary
OpenSSH is prone to a remote denial-of-service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     See references
Installation
path / port:       22/tcp
```

Impact
Exploiting this issue allows remote attackers to trigger denial-of- service conditions.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
OpenSSH 6.1 and prior.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

Vulnerability Detection Method

Compare the version retrieved from the banner with the affected range.
Details: `OpenSSH Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103939
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2010-5107
BID:58162
Other:
  URL:http://www.securityfocus.com/bid/58162
```

Medium (CVSS: 5.0)
NVT: OpenSSH Denial of Service Vulnerability - Jan16

Product detection result

```
cpe:/a:openbsd:openssh:5.3
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 denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     7.1p2
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read and application crash).

Solution

Solution type: VendorFix
Upgrade to OpenSSH version 7.1p2 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
OpenSSH versions before 7.1p2.

Vulnerability Insight
The flaw exists due to an error in 'ssh_packet_read_poll2' function within 'packet.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH Denial of Service Vulnerability - Jan16`
OID:1.3.6.1.4.1.25623.1.0.806671
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-1907
Other:
  URL:http://www.openssh.com/txt/release-7.1p2
   URL:https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a78
↪9277bb0733ca36e1c0
```

Medium (CVSS: 4.3)
NVT: OpenSSH Security Bypass Vulnerability

Product detection result

```
cpe:/a:openbsd:openssh:5.3
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary
This host is running OpenSSH and is prone to security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     6.9
Installation
path / port:       22/tcp
```

Impact
Successful exploitation will allow remote attackers to bypass intended access restrictions.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 6.9 or later.

Affected Software/OS

OpenSSH versions before 6.9.

Vulnerability Insight

The flaw is due to the refusal deadline was not checked within the x11_open_helper function.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `OpenSSH Security Bypass Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.806049

Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2015-5352
Other:
  URL:http://openwall.com/lists/oss-security/2015/07/01/10
```

Medium (CVSS: 5.0)

NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:5.3
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: 5.3
Fixed version:     7.8
Installation
path / port:       22/tcp
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2019-05-23T14:08:05+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

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

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary

The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result

```
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution

Solution type: Mitigation

Disable the weak encryption algorithms.

Vulnerability Insight

The ‘arcfour‘ cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

The ‘none‘ algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method

Check if remote ssh service supports Arcfour, none or CBC ciphers.

Details: `SSH Weak Encryption Algorithms Supported`

OID:1.3.6.1.4.1.25623.1.0.105611

Version used: `$Revision: 13581 $`

References

```
Other:
  URL:https://tools.ietf.org/html/rfc4253#section-6.3
   URL:https://www.kb.cert.org/vuls/id/958563
```

[return to 10.200.0.11]

2.1.4 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.

Affected Software/OS
TCP/IP v4

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.
Details: `TCP Sequence Number Approximation Reset Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902815
Version used: `$Revision: 11066 $`

References

```
CVE: CVE-2004-0230
BID:10183
Other:
  URL:http://xforce.iss.net/xforce/xfdb/15886
   URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html
   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:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx
   URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx
   URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
   URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
```

[return to 10.200.0.11]

2.1.5 Medium 53/tcp

Medium (CVSS: 5.0)
NVT: ISC BIND 'deny-answer-aliases' Denial of Service Vulnerability

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.13-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. Please see the references for more information.

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'.

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: `2019-07-24T08:39:52+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
```

Medium (CVSS: 4.3)
NVT: ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.9-P2
```

Impact
Successful exploitation will allow remote attackers to cause denial of service.

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.9-P2 or 9.10.4-P2 or 9.11.0b2 or later.

Affected Software/OS
ISC BIND versions 9.0.x through 9.9.9-P1, 9.10.0 through 9.10.4-P1, 9.11.0a3 through 9.11.0b1.

Vulnerability Insight
The flaw is due to an error in the BIND implementation of the lightweight resolver protocol which use alternate method to do name resolution.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.808751
Version used: `2019-07-05T09:54:18+0000`

Product Detection Result
Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2016-2775
BID:92037
Other:
  URL:https://kb.isc.org/article/AA-01393/74/CVE-2016-2775
```

Medium (CVSS: 4.0)
NVT: ISC BIND AXFR Response Denial of Service Vulnerability

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     Workaround
```

Impact

An authenticated remote attacker may cause a denial of service condition.

Solution

Solution type: Workaround

As a workaround operators of servers which accept untrusted zone data can mitigate their risk by operating an intermediary server whose role it is to receive zone data and then (if successful) re-distribute it to client-facing servers. Successful exploitation of the attack against the intermediary server may still occur but denial of service against the client-facing servers is significantly more difficult to achieve in this scenario.

Affected Software/OS

Version <= 9.10.4-P1

Vulnerability Insight

Primary DNS servers may cause a denial of service (secondary DNS server crash) via a large AXFR response, and possibly allows IXFR servers to cause a denial of service (IXFR client crash) via a large IXFR response and allows remote authenticated users to cause a denial of service (primary DNS server crash) via a large UPDATE message

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `ISC BIND AXFR Response Denial of Service Vulnerability`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.106118
Version used: `$Revision: 12096 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2016-6170
Other:
  URL:http://www.openwall.com/lists/oss-security/2016/07/06/3
   URL:https://lists.dns-oarc.net/pipermail/dns-operations/2016-July/015058.html
```

Medium (CVSS: 5.0)
NVT: ISC BIND Denial of Service Vulnerability

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.9-P4
```

Impact
An remote attacker may cause a denial of service condition.

Solution
Solution type: VendorFix
Upgrade to 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, 9.11.0-P1 or later.

Affected Software/OS
BIND 9

Vulnerability Insight
A defect in BIND's handling of responses containing a DNAME answer can cause a resolver to exit after encountering an assertion failure in db.c or resolver.c

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `ISC BIND Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106366
Version used: `2019-07-24T08:39:52+0000`

Product Detection Result
Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2016-8864
Other:
  URL:https://kb.isc.org/article/AA-01434
```

Medium (CVSS: 6.8)
NVT: ISC BIND Denial of Service Vulnerability - 02 - Jan16

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 remote denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.8-P3
```

Impact
Successful exploitation will allow remote attackers to cause denial of service.

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.8-P3 or 9.10.3-P3 or 9.9.8-S4 or later.

Affected Software/OS
ISC BIND versions 9.3.0 through 9.8.8, 9.9.0 through 9.9.8-P2, 9.9.3-S1 through 9.9.8-S3, 9.10.0 through 9.10.3-P2.

Vulnerability Insight
The flaw is due to an error in 'apl_42.c' script in ISC BIND.

. . . 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 Denial of Service Vulnerability - 02 - Jan16`
OID:1.3.6.1.4.1.25623.1.0.806996
Version used: `$Revision: 14181 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2015-8704
Other:
  URL:https://kb.isc.org/article/AA-01335
```

Medium (CVSS: 5.0)
NVT: ISC BIND Denial of Service Vulnerability - 03 - Jan16

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 remote denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.8-P2
```

Impact
Successful exploitation will allow remote attackers to cause denial of service.

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.8-P2 or 9.10.3-P2 or later.

Affected Software/OS
ISC BIND versions 9.0.x through 9.9.8, 9.10.0 through 9.10.3.

Vulnerability Insight
The flaw is due to an error in 'db.c' script in ISC BIND.

. . . 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 Denial of Service Vulnerability - 03 - Jan16`

OID:1.3.6.1.4.1.25623.1.0.806997

Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`

Method: `Determine which version of BIND name daemon is running`

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2015-8000
BID:79349
Other:
  URL:https://kb.isc.org/article/AA-01317
```

Medium (CVSS: 5.4)

NVT: ISC BIND Denial of Service Vulnerability - 05 - Jan16

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 remote denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.10.1-P2
```

Impact

Successful exploitation will allow remote attackers to cause denial of service.

Solution

Solution type: VendorFix

Upgrade to ISC BIND version 9.10.1-P2 or later.

Affected Software/OS

ISC BIND versions 9.7.0 through 9.10.1-P1.

Vulnerability Insight

The flaw is due to an error in Trust Anchor Management that can cause named to crash.

... 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 Denial of Service Vulnerability - 05 - Jan16`
OID:1.3.6.1.4.1.25623.1.0.806999
Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2015-1349
BID:72673
Other:
  URL:https://kb.isc.org/article/AA-01235
```

Medium (CVSS: 4.3)
NVT: ISC BIND DNS64 Denial of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.9-P8
```

Impact

Successful exploitation will allow remote attackers to cause denial-of-service against a server.

Solution

Solution type: VendorFix
Upgrade to ISC BIND version 9.9.9-P8 or 9.9.10rc3 or 9.10.5rc3 or 9.11.1rc3 or 9.9.9-S10 or 9.10.4-P8 or 9.11.0-P5 or later on Linux.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

ISC BIND 9.8.0 through 9.8.8-P1, 9.9.0 through 9.9.9-P6, 9.9.10b1 through 9.9.10rc1, 9.10.0 through 9.10.4-P6, 9.10.5b1 through 9.10.5rc1, 9.11.0 through 9.11.0-P3, 9.11.1b1 through 9.11.1rc1, 9.9.3-S1 through 9.9.9-S8 on Linux.

Vulnerability Insight

The flaw exists due to improper handling of queries when server is configured to use DNS64 and if the option 'break-dnssec yes' is in use.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `ISC BIND DNS64 Denial of Service Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.810976

Version used: `2019-07-24T08:39:52+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`

Method: `Determine which version of BIND name daemon is running`

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2017-3136
BID:97653
Other:
  URL:https://kb.isc.org/article/AA-01465/74/CVE-2017-3136
```

Medium (CVSS: 4.3)

NVT: ISC BIND lwresd Denial of Service Vulnerability

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.9-P2
```

Impact

An remote attacker may cause a denial of service condition.

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Upgrade to 9.9.9-P1, 9.10.4-P1, 9.11.0b1 or later.

Affected Software/OS
BIND 9

Vulnerability Insight
The lwresd component in BIND (which is not enabled by default) could crash while processing an overlong request name. This could lead to a denial of service.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ISC BIND lwresd Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106292
Version used: `2019-07-24T08:39:52+0000`

Product Detection Result
Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2016-2775
Other:
  URL:https://kb.isc.org/article/AA-01393
```

Medium (CVSS: 5.0)
NVT: ISC BIND NSID Request Denial of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.9.9-P3 or 9.10.4-P3 or 9.11.0
```

Impact
Successful exploitation will allow remote attackers to cause a denial of service.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Upgrade to ISC BIND version 9.9.9-P3 or 9.10.4-P3 or 9.11.0 or later on Linux.

Affected Software/OS

ISC BIND versions 9.1.0 through 9.8.4-P2 and 9.9.0 through 9.9.2-P2 on Linux.

Vulnerability Insight

The flaw exists due to mishandling of packets with malformed options. A remote attacker could use this flaw to make named exit unexpectedly with an assertion failure via a specially crafted DNS packet.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `ISC BIND NSID Request Denial of Service Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.809461

Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`

Method: `Determine which version of BIND name daemon is running`

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2016-2848
BID:93814
Other:
  URL:https://kb.isc.org/article/AA-01433/74/CVE-2016-2848
```

Medium (CVSS: 4.3)

NVT: ISC BIND Security Bypass Vulnerability

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)
```

Summary

A flaw was found in the way BIND handled TSIG authentication for dynamic updates. A remote attacker able to communicate with an authoritative BIND server could use this flaw to manipulate the contents of a zone, by forging a valid TSIG or SIG(0) signature for a dynamic update request.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     9.9.10-P2
```

Solution

Solution type: VendorFix

Update to version 9.9.10-P2, 9.10.5-P2, 9.11.1-P2, 9.9.10-S3, 9.10.5-S3 or later.

Affected Software/OS

ISC BIND versions 9.4.0-9.8.8, 9.9.0-9.9.10-P1, 9.10.0-9.10.5-P1, 9.11.0-9.11.1-P1, 9.9.3-S1-9.9.10-S2 and 9.10.5-S1-9.10.5-S2

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `ISC BIND Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106937
Version used: `2019-07-24T08:39:52+0000`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2017-3143
Other:
  URL:https://kb.isc.org/article/AA-01503/0
```

Medium (CVSS: 4.3)
NVT: ISC BIND Security Bypass Vulnerability (Remote)

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)
```

Summary

A flaw was found in the way BIND handled TSIG authentication for dynamic updates. A remote attacker able to communicate with an authoritative BIND server could use this flaw to manipulate the contents of a zone, by forging a valid TSIG or SIG(0) signature for a dynamic update request.

Vulnerability Detection Result

```
The server responded with the following signed request MAC:
e9b8e375d481254942f0d8c706b65e298ecad423a0bf56f291d0d412d2ef36d0
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Update to version 9.9.10-P2, 9.10.5-P2, 9.11.1-P2, 9.9.10-S3, 9.10.5-S3 or later.

Affected Software/OS

ISC BIND versions 9.4.0-9.8.8, 9.9.0-9.9.10-P1, 9.10.0-9.10.5-P1, 9.11.0-9.11.1-P1, 9.9.3-S1-9.9.10-S2 and 9.10.5-S1-9.10.5-S2

Vulnerability Detection Method

Sends a crafted update request for the TSIG key 'local-ddns' and checks if the response returns a signed MAC.

Details: `ISC BIND Security Bypass Vulnerability (Remote)`

OID:1.3.6.1.4.1.25623.1.0.106953

Version used: `$Revision: 13654 $`

Product Detection Result

Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`

Method: `Determine which version of BIND name daemon is running`

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2017-3143
Other:
  URL:https://kb.isc.org/article/AA-01503/0
   URL:http://www.synacktiv.ninja/ressources/CVE-2017-3143_BIND9_TSIG_dynamic_up
↪dates_vulnerability_Synacktiv.pdf
```

[return to 10.200.0.11]

2.1.6 Low 22/tcp

Low (CVSS: 2.1)

NVT: OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability

Product detection result

```
cpe:/a:openbsd:openssh:5.3
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

OpenSSH is prone to a local information-disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     5.8p2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       22/tcp
```

Impact

Local attackers can exploit this issue to obtain sensitive information. Information obtained may lead to further attacks.

Solution

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Versions prior to OpenSSH 5.8p2 are vulnerable.

Vulnerability Insight

ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105002
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2011-4327
BID:65674
Other:
  URL:http://www.securityfocus.com/bid/65674
   URL:http://www.openssh.com/txt/portable-keysign-rand-helper.adv
```

Low (CVSS: 3.5)
NVT: OpenSSH 'ssh_gssapi_parse_ename()' Function Denial of Service Vulnerability

Product detection result

```
cpe:/a:openbsd:openssh:5.3
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 denial-of-service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     See references
Installation
path / port:       22/tcp
```

Impact

Exploiting this issue allows remote attackers to trigger denial-of-service conditions due to excessive memory consumption.

Solution

Solution type: VendorFix

Updates are available. Please see the references for details.

Affected Software/OS

OpenSSH 5.8 and prior are vulnerable.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `OpenSSH 'ssh_gssapi_parse_ename()' Function Denial of Service Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.103937

Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2011-5000
BID:54114
Other:
  URL:http://www.securityfocus.com/bid/54114
```

Low (CVSS: 3.5)

NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability

Product detection result

```
cpe:/a:openbsd:openssh:5.3
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

The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite.
NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no nupported way to read an authorized_keys file in its own home directory.

Vulnerability Detection Result

```
Installed version: 5.3
Fixed version:     5.7
Installation
path / port:       22/tcp
```

Solution

Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS

OpenSSH before 5.7.

Vulnerability Detection Method

Details: `openssh-server Forced Command Handling Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103503
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:5.3`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2012-0814
BID:51702
Other:
  URL:http://www.securityfocus.com/bid/51702
   URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445
   URL:https://downloads.avaya.com/css/P8/documents/100161262
```

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary

The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution

Solution type: Mitigation

Disable the weak MAC algorithms.

Vulnerability Detection Method

Details: `SSH Weak MAC Algorithms Supported`

OID:1.3.6.1.4.1.25623.1.0.105610

Version used: `$Revision: 13581 $`

[return to 10.200.0.11]

2.1.7 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: 679124
Packet 2: 680189
```

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'

. . . continues on next page . . .

. . . continued from previous page . . .

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 the references for more information.

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: 14310 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
   URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152
```

[return to 10.200.0.11]

2.1.8 Low 53/tcp

Low (CVSS: 2.6)
NVT: ISC BIND NSEC3 Signed Zones Queries Denial of Service Vulnerability - Jan16

Product detection result

```
cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
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 denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Fixed version:     9.8.6-P2
```

Impact
Successful exploitation will allow remote attackers to cause denial of service.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.6-ESV-R10-P2 or 9.8.6-P2 or 9.9.4-P2 or later.

Affected Software/OS
ISC BIND versions 9.6.0.x through 9.6-ESV-R10-P1, 9.7 (all versions), 9.8.0 through 9.8.6-P1, 9.9.0 through 9.9.4-P1.

Vulnerability Insight
The flaw exists due to an error in 'query_findclosestnsec3' function in 'query.c' script in ISC BIND.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ISC BIND NSEC3 Signed Zones Queries Denial of Service Vulnerability - Jan16`
OID:1.3.6.1.4.1.25623.1.0.807216
Version used: `2019-07-05T09:54:18+0000`

Product Detection Result
Product: `cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References

```
CVE: CVE-2014-0591
BID:64801
Other:
  URL:https://kb.isc.org/article/AA-01078
```

[return to 10.200.0.11]

2.1.9 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
```

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2019-07-08T14:12:44+0000

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

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

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-h
↪ellman-group14-sha1,diffie-hellman-group1-sha1
server_host_key_algorithms:
ssh-rsa,ssh-dss
encryption_algorithms_client_to_server:
aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowf
↪ish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client:
aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowf
↪ish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
mac_algorithms_client_to_server:
hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com
↪,hmac-sha1-96,hmac-md5-96
mac_algorithms_server_to_client:
hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com
↪,hmac-sha1-96,hmac-md5-96
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Log Method
Details: SSH Protocol Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: $Revision: 13581 $

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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:
1.99
2.0
SSHv2 Fingerprint(s):
ssh-dss: 6e:aa:4c:70:13:21:86:52:4f:83:2f:83:0d:f1:92:d6
ssh-rsa: af:10:15:ab:a3:45:eb:25:50:82:02:a2:eb:06:c1:46
```

Log Method

Details: SSH Protocol Versions Supported
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: $Revision: 13594 $

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_5.3
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:    OpenVAS-VT
Password: OpenVAS-VT
```

Log Method

Details: SSH Server type and version
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: 2019-06-05T03:32:14+0000

[return to 10.200.0.11]

2.1.10 Log general/tcp

Log (CVSS: 0.0)
NVT: OpenSSH Detection Consolidation

Summary
The script reports a detected OpenSSH including the version number.

Vulnerability Detection Result

```
Detected OpenSSH Server
Version:       5.3
Location:      22/tcp
CPE:           cpe:/a:openbsd:openssh:5.3
Concluded from version/product identification result:
SSH-2.0-OpenSSH_5.3
```

Log Method
Details: `OpenSSH Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.108577
Version used: `2019-05-23T06:42:35+0000`

References

```
Other:
  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 NVTs 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:           Redhat Linux
Version:      6
CPE:          cpe:/o:redhat:linux:6
Found by NVT: 1.3.6.1.4.1.25623.1.0.108014 (DNS Server OS Identification)
Concluded from DNS server banner on port 53/tcp: 9.8.2rc1-RedHat-9.8.2-0.17.rc1.
↪el6
Setting key "Host/runs_unixoide" based on this information
```

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937

. . . continues on next page . . .

... continued from previous page ...

Version used: `2019-09-03T05:31:07+0000`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

Log (CVSS: 0.0)
NVT: Traceroute

Summary

A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 192.168.0.2 to 10.200.0.11:
192.168.0.2
10.200.0.11
```

Solution

Block unwanted packets from escaping your network.

Log Method

Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `$Revision: 10411 $`

[return to 10.200.0.11]

2.1.11 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary

The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

. . . continued from previous page . . .

Log Method

Details: `ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 10411 $`

References

```
CVE: CVE-1999-0524
Other:
  URL:http://www.ietf.org/rfc/rfc0792.txt
```

[return to 10.200.0.11]

2.1.12 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.

Vulnerability Detection Result

```
10.200.0.11|cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
10.200.0.11|cpe:/a:openbsd:openssh:5.3
10.200.0.11|cpe:/o:redhat:linux:6
```

Log Method

Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 14324 $`

References

```
Other:
  URL:http://cpe.mitre.org/
```

[return to 10.200.0.11]

2.1.13 Log 53/tcp

Log (CVSS: 0.0)
NVT: Determine which version of BIND name daemon is running

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code.

Vulnerability Detection Result

```
Detected Bind
Version:       9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Location:      53/tcp
CPE:           cpe:/a:isc:bind:9.8.2rc1.RedHat.9.8.2.0.17.rc1.el6
Concluded from version/product identification result:
9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6
```

Solution

Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts.

Vulnerability Insight

The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source.

Log Method

Details: `Determine which version of BIND name daemon is running`
OID:1.3.6.1.4.1.25623.1.0.10028
Version used: `$Revision: 10945 $`

Log (CVSS: 0.0)
NVT: DNS Server Detection (TCP)

Summary

A DNS Server is running at this Host. A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address.

Vulnerability Detection Result

```
The remote DNS server banner is:
9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6
```

Log Method

Details: `DNS Server Detection (TCP)`
OID:1.3.6.1.4.1.25623.1.0.108018
Version used: `$Revision: 13541 $`

[return to 10.200.0.11]