



CVE-2017-3139

Published on: 04/09/2019 12:00:00 AM UTC

Last Modified on: 05/14/2021 08:35:00 PM UTC

CVE-2017-3139

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Bind](#) from [Isc](#) contain the following vulnerability:

A denial of service flaw was found in the way BIND handled DNSSEC validation. A remote attacker could use this flaw to make named exit unexpectedly with an assertion failure via a specially crafted DNS response.

CVE-2017-3139 has been assigned by security-officer@isc.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: Red Hat - BIND version shipped in Red Hat Enterprise Linux 6

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
CVE-2017-3139 - Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	CONFIRM access.redhat.com/security/cve/cve-2017-3139

1447743 – (CVE-2017-3139) CVE-2017-3139 bind: assertion failure in DNSSEC validation

[Issue Tracking](#)[Third Party Advisory](#)[bugzilla.redhat.com](#)[text/html](#) **CONFIRM**[bugzilla.redhat.com/show_bug.cgi?](https://bugzilla.redhat.com/show_bug.cgi?id=1447743)

id=1447743

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[378245](#) Virtuozzo Linux Security Update for bind-chroot (VZLSA-2017:1202)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Isc	Bind	-	All	All	All
Application	Isc	Bind	-	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All

cpe:2.3:a:isc:bind:-:*:*:*:*:*:
cpe:2.3:a:isc:bind:-:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.2:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.4:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.5:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.6:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.2:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.4:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.5:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.6:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_eus:6.7:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_eus:6.7:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_tus:6.5:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_tus:6.6:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_tus:6.5:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_tus:6.6:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)