

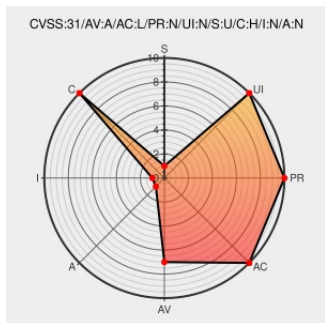


CVE-2020-25662

Published on: 11/05/2020 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:40:00 PM UTC

CVE-2020-25662

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

Certain versions of [Enterprise Linux](#) from [Redhat](#) contain the following vulnerability:

A Red Hat only CVE-2020-12352 regression issue was found in the way the Linux kernel's Bluetooth stack implementation handled the initialization of stack memory when handling certain AMP packets. This flaw allows a remote attacker in an adjacent range to leak small portions of stack memory on the system by sending specially crafted AMP packets. The highest threat from this vulnerability is to data confidentiality.

CVE-2020-25662 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Red Hat** - kernel version = **kernel-4.18.0-240.el8**

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

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

CVE References

Description	Tags	Link
-------------	------	------

1891484 – (CVE-2020-25662) CVE-2020-25662 kernel: Red Hat only CVE-2020-12352 regression	Issue Tracking Mitigation Vendor Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-25662
1891484 – (CVE-2020-25662) CVE-2020-25662 kernel: Red Hat only CVE-2020-12352 regression	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=1891484
BleedingTooth - Kernel Bluetooth vulnerabilities - CVE-2020-12351, CVE-2020-12352, and CVE-2020-24490 - Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	 CONFIRM access.redhat.com/security/vulnerabilities/BleedingTooth
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2020-25662
Red Hat Customer Portal	Mitigation Vendor Advisory access.redhat.com text/html	 CONFIRM access.redhat.com/security/cve/CVE-2020-12352
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2020:4686
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2020:4685
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 .		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	8.3	All	All	All
Operating System	Redhat	Enterprise Linux	8.3	All	All	All
cpe:2.3:o:redhat:enterprise_linux:8.3:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:8.3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous IDNext ID →		

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)