



# CVE-2020-25632

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-25632
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-03 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:20:00 UTC
<b>Description</b>	A flaw was found in grub2 in versions prior to 2.06. The rmmmod implementation allows the unloading of a module used as a

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Grub2</a>	All	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Grub2</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.2	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] Fedora 34 Update: shim-15.4-4 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 34 Update: shim-15.4-4 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
GRUB: Multiple vulnerabilities (GLSA 202104-05) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
1879577 – (CVE-2020-25632) CVE-2020-25632 grub2: Use-after-free in rmod command	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Trac
March 2021 Grub2 Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical,

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">178614</a> Debian Security Update for grub2 (DSA 4867-1)
<a href="#">178629</a> Debian Security Update for grub2 (DSA 4867-1)
<a href="#">198410</a> Ubuntu Security Notification for GRUB 2 vulnerabilities (USN-4992-1)
<a href="#">239315</a> Red Hat Update for shim (RHSA-2021:1734)
<a href="#">239469</a> Red Hat Update for fwupd (RHSA-2021:2566)
<a href="#">239494</a> Red Hat Update for shim and fwupd (RHSA-2021:2790)
<a href="#">239657</a> Red Hat Update for shim and fwupd (RHSA-2021:3675)
<a href="#">281363</a> Fedora Security Update for efi (FEDORA-2021-cab258a413)
<a href="#">352490</a> Amazon Linux Security Advisory for grub2: ALAS2-2021-1684
<a href="#">377367</a> Alibaba Cloud Linux Security Update for grub2 (ALINUX3-SA-2021:0026)
<a href="#">377414</a> Alibaba Cloud Linux Security Update for fwupd (ALINUX3-SA-2021:0048)
<a href="#">377548</a> Alibaba Cloud Linux Security Update for grub2 (ALINUX2-SA-2021:0020)
<a href="#">502730</a> Alpine Linux Security Update for grub
<a href="#">670282</a> EulerOS Security Update for grub2 (EulerOS-SA-2021-1794)
<a href="#">670324</a> EulerOS Security Update for grub2 (EulerOS-SA-2021-1900)
<a href="#">670349</a> EulerOS Security Update for grub2 (EulerOS-SA-2021-1875)
<a href="#">670376</a> EulerOS Security Update for grub2 (EulerOS-SA-2021-1948)
<a href="#">670398</a> EulerOS Security Update for grub2 (EulerOS-SA-2021-1927)
<a href="#">670618</a> EulerOS Security Update for grub2 (EulerOS-SA-2021-2376)
<a href="#">670931</a> EulerOS Security Update for grub2 (EulerOS-SA-2021-1875)
<a href="#">710015</a> Gentoo Linux GRUB Multiple Vulnerabilities (GLSA 202104-05)
<a href="#">730228</a> McAfee Web Gateway Multiple Vulnerabilities (WP-3445, WP-3483, WP-3527, WP-3528, WP-3547, WP-3584,WP-3589,WP-3611)
<a href="#">750300</a> OpenSUSE Security Update for grub2 (openSUSE-SU-2021:0462-1)
<a href="#">900055</a> CBL-Mariner Linux Security Update for grub2 2.06~rc1
<a href="#">901929</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6461-1)
<a href="#">902823</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3931)
<a href="#">906145</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3931-1)
<a href="#">906270</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6461-2)

[940046](#) AlmaLinux Security Update for fwupd (ALSA-2021:2566)

[940314](#) AlmaLinux Security Update for shim (ALSA-2021:1734)

[940320](#) AlmaLinux Security Update for grub2 (ALSA-2021:0696)

[960461](#) Rocky Linux Security Update for shim (RLSA-2021:1734)

[960826](#) Rocky Linux Security Update for fwupd (RLSA-2021:2566)

© [CVE.report](#) 2026 |

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](#)