



CVE-2021-20225

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

Summary

CVE	CVE-2021-20225
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-03 17:15:00 UTC
Updated	2023-11-07 03:29:00 UTC
Description	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-alloc

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Gnu	Grub2	All	All	All	All
Application	Gnu	Grub2	All	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	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 Aus	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
[SECURITY] Fedora 34 Update: shim-15.4-4 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 34 Update: shim-15.4-4 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
1924696 – (CVE-2021-20225) CVE-2021-20225 grub2: Heap out-of-bounds write in short form option parser	MISC	bugzilla.redhat.com
GRUB: Multiple vulnerabilities (GLSA 202104-05) — Gentoo security	GENTOO	security.gentoo.org
March 2021 Grub2 Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

178614 Debian Security Update for grub2 (DSA 4867-1)
178629 Debian Security Update for grub2 (DSA 4867-1)
179693 Debian Security Update for grub2 (CVE-2021-20225)
198410 Ubuntu Security Notification for GRUB 2 vulnerabilities (USN-4992-1)
239315 Red Hat Update for shim (RHSA-2021:1734)
239469 Red Hat Update for fwupd (RHSA-2021:2566)
239494 Red Hat Update for shim and fwupd (RHSA-2021:2790)
239657 Red Hat Update for shim and fwupd (RHSA-2021:3675)
281363 Fedora Security Update for efi (FEDORA-2021-cab258a413)
352490 Amazon Linux Security Advisory for grub2: ALAS2-2021-1684
377367 Alibaba Cloud Linux Security Update for grub2 (ALINUX3-SA-2021:0026)
377414 Alibaba Cloud Linux Security Update for fwupd (ALINUX3-SA-2021:0048)
377548 Alibaba Cloud Linux Security Update for grub2 (ALINUX2-SA-2021:0020)
502730 Alpine Linux Security Update for grub
670282 EulerOS Security Update for grub2 (EulerOS-SA-2021-1794)
670324 EulerOS Security Update for grub2 (EulerOS-SA-2021-1900)
670349 EulerOS Security Update for grub2 (EulerOS-SA-2021-1875)
670376 EulerOS Security Update for grub2 (EulerOS-SA-2021-1948)
670398 EulerOS Security Update for grub2 (EulerOS-SA-2021-1927)
670618 EulerOS Security Update for grub2 (EulerOS-SA-2021-2376)
670931 EulerOS Security Update for grub2 (EulerOS-SA-2021-1875)
710015 Gentoo Linux GRUB Multiple Vulnerabilities (GLSA 202104-05)
730228 McAfee Web Gateway Multiple Vulnerabilities (WP-3445, WP-3483, WP-3527, WP-3528, WP-3547, WP-3584, WP-3589, WP-3611)
750300 OpenSUSE Security Update for grub2 (openSUSE-SU-2021:0462-1)
900055 CBL-Mariner Linux Security Update for grub2 2.06~rc1
901747 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6465-1)
903289 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3934)
906216 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3934-1)

906321 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6465-2)
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](#)