CVE-2020-27779

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-27779
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 03:21:00 UTC
Description	A flaw was found in grub2 in versions prior to 2.06. The cutmem command does not honor secure boot locking allowing an

Risk And Classification

Problem Types: NVD-CWE-Other

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
[SECURITY] Fedora 34 Update: shim-15.4-4 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 34 Update: shim-15.4-4 - package-announce - Fedora Mailing-Lists
GRUB: Multiple vulnerabilities (GLSA 202104-05) — Gentoo security
March 2021 Grub2 Vulnerabilities in NetApp Products | NetApp Product Security
1900698 – (CVE-2020-27779) CVE-2020-27779 grub2: cutmem command allows privileged user to remove memory regions when Secure Bo
CVE Program record
NVD vulnerability detail

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)

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)

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)

670460 EulerOS Security Update for grub2 (EulerOS-SA-2021-2218)

670618 EulerOS Security Update for grub2 (EulerOS-SA-2021-2376)

670931 EulerOS Security Update for grub2 (EulerOS-SA-2021-1875)

672656 EulerOS Security Update for grub2 (EulerOS-SA-2023-1386)

672662 EulerOS Security Update for grub2 (EulerOS-SA-2023-1358)

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

901781 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6464-1)

902832 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3946)

906098 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3946-1)

906457 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6464-2)

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)