CVE-2020-15707

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-15707
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-29 18:15:00 UTC
Updated	2021-09-13 14:25:00 UTC
Description	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2

Risk And Classification

Problem Types: CWE-362 | CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Gnu	Grub2	All	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	All	All	All

Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows 10	2004	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows 10	2004	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	2004	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	2004	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	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
Application	Redhat	Enterprise Linux Atomic Host	-	All	All	All
Application	Redhat	Enterprise Linux Atomic Host	-	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	12	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	15	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	12	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	15	All	All	All

References

Reference	Source	Link	Tag
oss-security - multiple secure boot grub2 and linux kernel vulnerabilities	MLIST	www.openwall.com	Mail
oss-security - multiple secure boot grub2 and linux kernel vulnerabilities	CONFIRM	www.openwall.com	Mail
[SECURITY PATCH 00/28] Multiple GRUB2 vulnerabilities - BootHole	CONFIRM	lists.gnu.org	Issu
Security Vulnerability: "Boothole" grub2 UEFI secure boot lockdown bypass | Support | SUSE	SUSE	www.suse.com	Thir
SecurityTeam/KnowledgeBase/GRUB2SecureBootBypass - Ubuntu Wiki	UBUNTU	wiki.ubuntu.com	Thir
July 2020 Grub2 Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Thir
portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011	CONFIRM	portal.msrc.microsoft.com	Thir
Debian -- Security Information -- DSA-4735-1 grub2	DEBIAN	www.debian.org	Thir
SUSE addresses BootHole security exposure - SUSE Communities	SUSE	www.suse.com	Thir
[security-announce] openSUSE-SU-2020:1168-1: important: Security update	SUSE	lists.opensuse.org	
Debian -- GRUB2 UEFI SecureBoot vulnerability - 'BootHole'	DEBIAN	www.debian.org	Thir
[security-announce] openSUSE-SU-2020:1169-1: important: Security update	SUSE	lists.opensuse.org	
GRUB: Multiple vulnerabilities (GLSA 202104-05) — Gentoo security	GENTOO	security.gentoo.org	
USN-4432-1: GRUB 2 vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
Boot Hole Vulnerability - GRUB 2 boot loader - CVE-2020-10713 - Red Hat Customer Portal	REDHAT	access.redhat.com	Thir
USN-4432-1: GRUB 2 vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	ubuntu.com	Thir
There's a Hole in the Boot - Eclypsium	CONFIRM	www.eclypsium.com	Expl
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

Vendor Comments And Credit

Discovery Credit

Discovery Credit

LEGACY: Colin Watson

LEGACY: Chris Coulson

Legacy QID Mappings

377345 Alibaba Cloud Linux Security Update for grub2 (ALINUX3-SA-2022:0064)

377533 Alibaba Cloud Linux Security Update for grub2 (ALINUX2-SA-2020:0108)

502730 Alpine Linux Security Update for grub

710015 Gentoo Linux GRUB Multiple Vulnerabilities (GLSA 202104-05)

900175 CBL-Mariner Linux Security Update for grub2 2.02

903638 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1828)