



# CVE-2020-15707

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

## Summary

<b>CVE</b>	CVE-2020-15707
<b>State</b>	PUBLIC
<b>Assigner</b>	security@ubuntu.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-07-29 18:15:00 UTC
<b>Updated</b>	2021-09-13 14:25:00 UTC
<b>Description</b>	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	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Grub2</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10</a>	1607	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10</a>	1709	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10</a>	1803	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10</a>	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	<a href="http://www.openwall.com">www.openwall.com</a>	Mail
oss-security - multiple secure boot grub2 and linux kernel vulnerabilities	CONFIRM	<a href="http://www.openwall.com">www.openwall.com</a>	Mail
[SECURITY PATCH 00/28] Multiple GRUB2 vulnerabilities - BootHole	CONFIRM	<a href="http://lists.gnu.org">lists.gnu.org</a>	Issu
Security Vulnerability: "Boothole" grub2 UEFI secure boot lockdown bypass   Support   SUSE	SUSE	<a href="http://www.suse.com">www.suse.com</a>	Thir
SecurityTeam/KnowledgeBase/GRUB2SecureBootBypass - Ubuntu Wiki	UBUNTU	<a href="http://wiki.ubuntu.com">wiki.ubuntu.com</a>	Thir
July 2020 Grub2 Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="http://security.netapp.com">security.netapp.com</a>	Thir
portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011	CONFIRM	<a href="http://portal.msrc.microsoft.com">portal.msrc.microsoft.com</a>	Thir
Debian -- Security Information -- DSA-4735-1 grub2	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Thir
SUSE addresses BootHole security exposure - SUSE Communities	SUSE	<a href="http://www.suse.com">www.suse.com</a>	Thir
[security-announce] openSUSE-SU-2020:1168-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
Debian -- GRUB2 UEFI SecureBoot vulnerability - 'BootHole'	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Thir
[security-announce] openSUSE-SU-2020:1169-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
GRUB: Multiple vulnerabilities (GLSA 202104-05) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
USN-4432-1: GRUB 2 vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="http://usn.ubuntu.com">usn.ubuntu.com</a>	
Boot Hole Vulnerability - GRUB 2 boot loader - CVE-2020-10713 - Red Hat Customer Portal	REDHAT	<a href="http://access.redhat.com">access.redhat.com</a>	Thir
USN-4432-1: GRUB 2 vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="http://ubuntu.com">ubuntu.com</a>	Thir
There's a Hole in the Boot - Eclipsium	CONFIRM	<a href="http://www.eclipsium.com">www.eclipsium.com</a>	Exp
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canc
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canc

## Vendor Comments And 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)© [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](#)