CVE-2018-16865

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-16865
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-11 21:29:00 UTC
Updated	2023-02-13 04:52:00 UTC
Description	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered i

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	18.10	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	18.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Freedesktop	Systemd	All	All	All	All
Application	Oracle	Communications Session Border Controller	8.0.0	All	All	All
Application	Oracle	Communications Session Border Controller	8.1.0	All	All	All
Application	Oracle	Communications Session Border Controller	8.2.0	All	All	All
Application	Oracle	Communications Session Border Controller	8.0.0	All	All	All
Application	Oracle	Communications Session Border Controller	8.1.0	All	All	All
Application	Oracle	Communications Session Border Controller	8.2.0	All	All	All

Application	Oracle	Enterprise Communications Broker	3.0.0	All	All	All
Application	Oracle	Enterprise Communications Broker	3.1.0	All	All	All
Application	Oracle	Enterprise Communications Broker	3.0.0	All	All	All
Application	Oracle	Enterprise Communications Broker	3.1.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	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
Application	Systemd Project	Systemd	All	All	All	All

References

Reference	Source	Link
systemd-journald CVE-2018-16865 Stack Buffer Overflow Vulnerability	BID	www.securityf
1653861 – (CVE-2018-16865) CVE-2018-16865 systemd: stack overflow when receiving many journald entries	MISC	bugzilla.redha
Bugtraq: Re: System Down: A systemd-journald exploit	BUGTRAQ	seclists.org
1653861 – (CVE-2018-16865) CVE-2018-16865 systemd: stack overflow when receiving many journald entries	CONFIRM	bugzilla.redha
Debian -- Security Information -- DSA-4367-1 systemd	DEBIAN	www.debian.o
oss-security - Re: System Down: A systemd-journald exploit	MLIST	www.openwall
Red Hat Customer Portal	REDHAT	access.redhat
Red Hat Customer Portal	REDHAT	access.redhat
January 2019 Systemd-journald Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netap

Red Hat Customer Portal	REDHAT	access.redhat
Red Hat Customer Portal	REDHAT	access.redhat
Red Hat Customer Portal	REDHAT	access.redhat
CVE-2018-16865 - Red Hat Customer Portal	MISC	access.redhat
oss-security - CVE-2021-33910: Denial of service (stack exhaustion) in systemd (PID 1)	MLIST	www.openwall
USN-3855-1: systemd vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.co
System Down: A systemd-journald Exploit ≈ Packet Storm	MISC	packetstormse
Red Hat Customer Portal	REDHAT	access.redhat
Full Disclosure: Re: System Down: A systemd-journald exploit	FULLDISC	seclists.org
Red Hat Customer Portal	REDHAT	access.redhat
[SECURITY] [DLA 1639-1] systemd security update	MLIST	lists.debian.or
systemd: Multiple vulnerabilities (GLSA 201903-07) — Gentoo security	GENTOO	security.gento
www.qualys.com/2019/01/09/system-down/system-down.txt	MISC	www.qualys.c
Oracle Critical Patch Update Advisory - April 2019	MISC	www.oracle.c
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

900013 CBL-Mariner Linux Security Update for systemd 239

902820 Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (1791)