CVE-2018-16866

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-16866
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-11 19:29:00 UTC
Updated	2023-02-13 04:52:00 UTC
Description	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'.

Risk And Classification

Problem Types: CWE-200 | CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Upd
Operating System	Canonical	Ubuntu Linux	16.04	All
Operating System	Canonical	Ubuntu Linux	18.04	All
Operating System	Canonical	Ubuntu Linux	18.10	All
Operating System	Canonical	Ubuntu Linux	16.04	All
Operating System	Canonical	Ubuntu Linux	18.04	All
Operating System	Canonical	Ubuntu Linux	18.10	All
Operating System	Debian	Debian Linux	9.0	All
Operating System	Debian	Debian Linux	9.0	All
Application	Freedesktop	Systemd	All	All
Application	Netapp	Active Iq Performance Analytics Services	-	All
Application	Netapp	Active Iq Performance Analytics Services	-	All
Application	Netapp	Element Software	All	All
Application	Netapp	Element Software	All	All
Operating System	Redhat	Enterprise Linux	7.6	All
Operating System	Redhat	Enterprise Linux Compute Node Eus	7.6	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.6	All

Operating System	Redhat	Enterprise Linux For Ibm Z Systems Structure A	7_s390x	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	7.0	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.6	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	7.0	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.6	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	7.0	All
Operating System	Redhat	Enterprise Linux Server	7.0	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	7.4	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	7.6	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	7.4	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	7.6	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All
Application	Systemd Project	Systemd	All	All

References

Reference	Source	Link
systemd-journald CVE-2018-16866 Out-Of-Bounds Read Information Disclosure Vulnerability	BID	www.s
Red Hat Customer Portal	REDHAT	access
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access
Bugtraq: Re: System Down: A systemd-journald exploit	BUGTRAQ	seclists
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access
Red Hat Customer Portal	REDHAT	access
Debian -- Security Information -- DSA-4367-1 systemd	DEBIAN	www.d
Red Hat Customer Portal	REDHAT	access
oss-security - Re: System Down: A systemd-journald exploit	MLIST	www.o
January 2019 Systemd-journald Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	securit
1653867 – (CVE-2018-16866) CVE-2018-16866 systemd: out-of-bounds read when parsing a crafted syslog message	MISC	bugzill
USN-3855-1: systemd vulnerabilities | Ubuntu security notices	UBUNTU	usn.ub
System Down: A systemd-journald Exploit ≈ Packet Storm	MISC	packet
Full Disclosure: Re: System Down: A systemd-journald exploit	FULLDISC	seclists
systemd: Multiple vulnerabilities (GLSA 201903-07) — Gentoo security	GENTOO	securit

CVE-2018-16866 - Red Hat Customer Portal	MISC	access
www.qualys.com/2019/01/09/system-down/system-down.txt	MISC	www.q
1653867 – (CVE-2018-16866) CVE-2018-16866 systemd: out-of-bounds read when parsing a crafted syslog message	CONFIRM	bugzill
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

352381 Amazon Linux Security Advisory for systemd: ALAS2-2021-1647

900013 CBL-Mariner Linux Security Update for systemd 239

902836 Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (1798)