



# CVE-2018-16866

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

## Summary

<b>CVE</b>	CVE-2018-16866
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-01-11 19:29:00 UTC
<b>Updated</b>	2023-02-13 04:52:00 UTC
<b>Description</b>	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	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All
Application	<a href="#">Freedesktop</a>	<a href="#">Systemd</a>	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Performance Analytics Services</a>	-	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Performance Analytics Services</a>	-	All
Application	<a href="#">Netapp</a>	<a href="#">Element Software</a>	All	All
Application	<a href="#">Netapp</a>	<a href="#">Element Software</a>	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Compute Node Eus</a>	7.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems Eus</a>	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	<a href="#">www.s</a>
Red Hat Customer Portal	REDHAT	<a href="#">access</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access</a>
Bugtraq: Re: System Down: A systemd-journald exploit	BUGTRAQ	<a href="#">seclists</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access</a>
Red Hat Customer Portal	REDHAT	<a href="#">access</a>
Debian -- Security Information -- DSA-4367-1 systemd	DEBIAN	<a href="#">www.d</a>
Red Hat Customer Portal	REDHAT	<a href="#">access</a>
oss-security - Re: System Down: A systemd-journald exploit	MLIST	<a href="#">www.o</a>
January 2019 Systemd-journald Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">securit</a>
1653867 – (CVE-2018-16866) CVE-2018-16866 systemd: out-of-bounds read when parsing a crafted syslog message	MISC	<a href="#">bugzilla</a>
USN-3855-1: systemd vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ub</a>
System Down: A systemd-journald Exploit ≈ Packet Storm	MISC	<a href="#">packet</a>
Full Disclosure: Re: System Down: A systemd-journald exploit	FULLDISC	<a href="#">seclists</a>
systemd: Multiple vulnerabilities (GLSA 201903-07) — Gentoo security	GENTOO	<a href="#">securit</a>

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

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)

© [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](#)