



# CVE-2018-16864

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-16864
<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 20:29:00 UTC
<b>Updated</b>	2023-02-13 04:51:00 UTC
<b>Description</b>	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in

## Risk And Classification

**Problem Types:** CWE-770

## 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>	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>	18.10	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>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Freedesktop</a>	<a href="#">Systemd</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Session Border Controller</a>	8.0.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Session Border Controller</a>	8.1.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Session Border Controller</a>	8.2.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Session Border Controller</a>	8.0.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Session Border Controller</a>	8.1.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Session Border Controller</a>	8.2.0	All	All	All

Application	<a href="#">Oracle</a>	<a href="#">Enterprise Communications Broker</a>	3.0.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Enterprise Communications Broker</a>	3.1.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Enterprise Communications Broker</a>	3.0.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Enterprise Communications Broker</a>	3.1.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Application	<a href="#">Systemd Project</a>	<a href="#">Systemd</a>	All	All	All	All

## References

Reference	Source
1653855 – (CVE-2018-16864) CVE-2018-16864 systemd: stack overflow when calling syslog from a command with long cmdline	CONFIRM
CVE-2018-16864 - Red Hat Customer Portal	MISC
Debian -- Security Information -- DSA-4367-1 systemd	DEBIAN
Debian -- Security Information -- DSA-4367-1 systemd	DEBIAN

Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
January 2019 Systemd-journald Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
oss-security - CVE-2021-33910: Denial of service (stack exhaustion) in systemd (PID 1)	MLIST
systemd-journald CVE-2018-16864 Stack-Based Buffer Overflow Vulnerability	BID
USN-3855-1: systemd vulnerabilities   Ubuntu security notices	UBUNTU
1653855 – (CVE-2018-16864) CVE-2018-16864 systemd: stack overflow when calling syslog from a command with long cmdline	MISC
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
[SECURITY] [DLA 1639-1] systemd security update	MLIST
systemd: Multiple vulnerabilities (GLSA 201903-07) — Gentoo security	GENTOO
www.qualys.com/2019/01/09/system-down/system-down.txt	MISC
Oracle Critical Patch Update Advisory - April 2019	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[900013](#) CBL-Mariner Linux Security Update for systemd 239

[903037](#) Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (1796)

© [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](#)