



# CVE-2020-15862

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

## Summary

<b>CVE</b>	CVE-2020-15862
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-08-20 01:17:00 UTC
<b>Updated</b>	2023-11-22 16:15:00 UTC
<b>Description</b>	Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides

## Risk And Classification

**Problem Types:** CWE-269

## 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>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	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>	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>	18.04	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>	12.04	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
Application	<a href="#">Net-snmp</a>	<a href="#">Net-snmp</a>	All	All	All	All
Application	<a href="#">Net-snmp</a>	<a href="#">Net-snmp</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All

Application	<a href="#">Netapp</a>	<a href="#">Smi-s Provider</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All

## References

Reference	Source	Link
August 2020 Net-SNMP Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
make the extend mib read-only by default · net-snmp/net-snmp@77f6c60 · GitHub	CONFIRM	<a href="https://github.com">github.com</a>
Net-SNMP: Multiple vulnerabilities (GLSA 202008-12) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
snmpd: Disable extend mib Closes: #965166 (fad87254) · Commits · Debian / net-snmp · GitLab	CONFIRM	<a href="https://salsa.debian.org">salsa.debian.org</a>
#965166 - snmpd privilege escalation - Debian Bug report logs	MISC	<a href="https://bugs.debian.org">bugs.debian.org</a>
USN-4471-1: Net-SNMP vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
CVE-2020-15862	MISC	<a href="https://security-tracker.debian.org">security-tracker.debian.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">352292</a> Amazon Linux Security Update for net-snmp: AL2012-2021-333
<a href="#">376248</a> IBM Spectrum Control Multiple Vulnerabilities (6359903,6359899,6359901)
<a href="#">376926</a> Alibaba Cloud Linux Security Update for net-snmp (ALINUX3-SA-2021:0005)
<a href="#">377196</a> Alibaba Cloud Linux Security Update for net-snmp (ALINUX2-SA-2020:0190)
<a href="#">591311</a> Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)
<a href="#">751561</a> SUSE Enterprise Linux Security Update for net-snmp (SUSE-SU-2021:4191-1)
<a href="#">751579</a> SUSE Enterprise Linux Security Update for net-snmp (SUSE-SU-2022:0030-1)
<a href="#">751589</a> SUSE Enterprise Linux Security Update for net-snmp (SUSE-SU-2022:0050-1)
<a href="#">751591</a> OpenSUSE Security Update for net-snmp (openSUSE-SU-2022:0050-1)
<a href="#">751907</a> SUSE Enterprise Linux Security Update for net-snmp (SUSE-SU-2022:0050-2)
<a href="#">940324</a> AlmaLinux Security Update for net-snmp (ALSA-2020:5480)

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](#)**