



CVE-2020-27827

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-27827 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-03-18 17:15:00 UTC |
| Updated | 2023-11-26 11:15:00 UTC |
| Description | A flaw was found in multiple versions of OpenvSwitch. Specially crafted LLDP packets can cause memory to be lost when a |

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|---|---------|--------|---------|----------|
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Application | Lldpd Project | Lldpd | All | All | All | All |
| Application | Openvswitch | Openvswitch | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |
| Application | Redhat | Openshift Container Platform | 4.0 | All | All | All |
| Application | Redhat | Openstack | 10 | All | All | All |
| Application | Redhat | Openstack | 13 | All | All | All |
| Application | Redhat | Openstack | 13.0 | All | All | All |
| Application | Redhat | Virtualization | 4.0 | All | All | All |
| Hardware | Siemens | Simatic Hmi Unified Comfort Panels | - | All | All | All |
| Operating System | Siemens | Simatic Hmi Unified Comfort Panels Firmware | All | All | All | All |
| Hardware | Siemens | Simatic Net Cp 1243-1 | - | All | All | All |
| Operating System | Siemens | Simatic Net Cp 1243-1 Firmware | - | All | All | All |
| Hardware | Siemens | Simatic Net Cp 1243-8 Irc | - | All | All | All |
| Operating System | Siemens | Simatic Net Cp 1243-8 Irc Firmware | - | All | All | All |
| Hardware | Siemens | Simatic Net Cp 1542sp-1 | - | All | All | All |

| | | | | | | |
|------------------|---------|--------------------------------------|-----|-----|-----|-----|
| Operating System | Siemens | Simatic Net Cp 1542sp-1 Firmware | - | All | All | All |
| Hardware | Siemens | Simatic Net Cp 1542sp-1 Irc | - | All | All | All |
| Operating System | Siemens | Simatic Net Cp 1542sp-1 Irc Firmware | - | All | All | All |
| Hardware | Siemens | Simatic Net Cp 1543-1 | - | All | All | All |
| Operating System | Siemens | Simatic Net Cp 1543-1 Firmware | - | All | All | All |
| Hardware | Siemens | Simatic Net Cp 1543sp-1 | - | All | All | All |
| Operating System | Siemens | Simatic Net Cp 1543sp-1 Firmware | - | All | All | All |
| Hardware | Siemens | Simatic Net Cp 1545-1 | - | All | All | All |
| Operating System | Siemens | Simatic Net Cp 1545-1 Firmware | - | All | All | All |
| Hardware | Siemens | Sinumerik One | - | All | All | All |
| Operating System | Siemens | Sinumerik One Firmware | All | All | All | All |
| Hardware | Siemens | Tim 1531 Irc | - | All | All | All |
| Operating System | Siemens | Tim 1531 Irc Firmware | All | All | All | All |

References

| Reference | Source | Link |
|---|---------|--------------------------|
| [SECURITY] Fedora 38 Update: lldpd-1.0.16-1.fc38 - package-announce - Fedora Mailing-Lists | | lists.fe |
| 1921438 – (CVE-2020-27827) CVE-2020-27827 lldp/openswitch: denial of service via externally triggered memory leak | MISC | bugzi |
| cert-portal.siemens.com/productcert/pdf/ssa-941426.pdf | CONFIRM | cert-p |
| [SECURITY] Fedora 37 Update: lldpd-1.0.16-1.fc37 - package-announce - Fedora Mailing-Lists | | lists.fe |
| [ovs-dev] [ADVISORY] CVE-2020-27827: lldp: Externally triggered memory leak. | MISC | mail.c |
| Open vSwitch: Multiple Vulnerabilities (GLSA 202311-16) — Gentoo security | | secur |
| [SECURITY] Fedora 36 Update: lldpd-1.0.16-1.fc36 - package-announce - Fedora Mailing-Lists | | lists.fe |
| [SECURITY] Fedora 37 Update: lldpd-1.0.16-1.fc37 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fe |
| [SECURITY] Fedora 36 Update: lldpd-1.0.16-1.fc36 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fe |
| [SECURITY] Fedora 38 Update: lldpd-1.0.16-1.fc38 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fe |
| Siemens Industrial Products LLDP CISA | MISC | us-ce |
| CVE Program record | CVE.ORG | www. |
| NVD vulnerability detail | NVD | nvd.n |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[174589](#) SUSE Enterprise Linux Security Update for openswitch (SUSE-SU-2021:0300-1)

[181728](#) Debian Security Update for lldpd (DLA 3388-1)

| |
|--|
| 181730 Debian Security Update for lldpd (DLA 3389-1) |
| 239427 Red Hat Update for Red Hat OpenStack Platform 13.0 (RHSA-2021:2456) |
| 281603 Fedora Security Update for dpdk (FEDORA-2021-fba11d37ee) |
| 283901 Fedora Security Update for lldpd (FEDORA-2023-c0c184a019) |
| 283902 Fedora Security Update for lldpd (FEDORA-2023-3e4feeadee) |
| 284191 Fedora Security Update for lldpd (FEDORA-2023-88991d2713) |
| 501072 Alpine Linux Security Update for lldpd |
| 501655 Alpine Linux Security Update for openvswitch |
| 505197 Alpine Linux Security Update for openvswitch |
| 591139 Siemens Industrial Products LLDP (Update D) Multiple Vulnerabilities (icsa-21-194-07, SSA-941426) |
| 710800 Gentoo Linux Open vSwitch Multiple Vulnerabilities (GLSA 202311-16) |
| 750374 OpenSUSE Security Update for openvswitch (openSUSE-SU-2021:0239-1) |
| 900147 CBL-Mariner Linux Security Update for openvswitch 2.12.0 |
| 901842 Common Base Linux Mariner (CBL-Mariner) Security Update for lldpd (7284) |
| 902651 Common Base Linux Mariner (CBL-Mariner) Security Update for lldpd (10443) |
| 903161 Common Base Linux Mariner (CBL-Mariner) Security Update for openvswitch (4019) |
| 903813 Common Base Linux Mariner (CBL-Mariner) Security Update for lldpd (10443-1) |

© [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](#)