



CVE-2020-29379

Published on: 11/28/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-29379

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N



Certain versions of **V1600d-mini** from **Vsolcn** contain the following vulnerability:

An issue was discovered on V-SOL V1600D4L V1.01.49 and V1600D-MINI V1.01.48 OLT devices. During the process of updating the firmware, the update script starts a telnetd -l /bin/sh process that does not require authentication for TELNET access.

CVE-2020-29379 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Full Disclosure: Multiple vulnerabilities found in V-SOL OLTs	Exploit Mailing List Third Party Advisory seclists.org text/html	MISC seclists.org/fulldisclosure/2020/Jul/14

There are currently no QIDs associated with this CVE

No vendor comments have been submitted for this CVE

Next ID→

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](#)