



Perle IOLAN STS/SCS Authenticated Command Injection via 'shell ps'

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

Summary

CVE	CVE-2026-23759
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-17 16:16:20 UTC
Updated	2026-05-01 15:23:27 UTC
Description	Perle IOLAN STS/SCS terminal server models with firmware versions prior to 6.0 allow authenticated OS command injection

Risk And Classification

Primary CVSS: v4.0 8.6 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.001950000 probability, percentile 0.411140000 (date 2026-05-05)

Problem Types: CWE-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA
4.0	CNA	CVSS	8.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Perle Systems	IOLAN STS	affected 6.0 semver	Not specified
CNA	Perle Systems	IOLAN SCS	affected 6.0 semver	Not specified

References

Reference	Source	Link	
www.perle.com/support_services/documentation_pdfs/iolan_scs-sds-sts_ug.pdf	disclosure@vulncheck.com	www.perle.com	1
www.vulncheck.com/advisories/perle-iolan-sts-scs-authenticated-command-injectio...	disclosure@vulncheck.com	www.vulncheck.com	
www.perle.com/downloads/server_sds_sts_rackmount.shtml	disclosure@vulncheck.com	www.perle.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

Vendor Comments And Credit

Discovery Credit

CNA: Victor A. Morales, Senior Pentester Team Leader, GM Sectec, Corp. (en)

CNA: Omar Crespo, Pentester, GM Sectec, Corp. (en)

CNA: VulnCheck (en)

Additional Advisory Data

Solutions

CNA: The vendor has stated that the IOLAN SCG and SCR models do not contain this vulnerable functionality.

There are currently no legacy QID mappings associated with this CVE.

© 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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org/). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report