



CVE-2018-0059

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

Summary

CVE	CVE-2018-0059
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-10 18:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A persistent cross-site scripting vulnerability in the graphical user interface of ScreenOS may allow a remote authenticated

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Netscreen Screenos	6.3.0	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r1	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r10	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r11	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r12	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r13	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r14	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r15	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r16	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r17	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r18	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r19	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r2	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r21	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r22	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r23	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r23b1	All	All	All

Operating System	Juniper	Netscreen Screenos	6.3.0r8	All	All	All
Operating System	Juniper	Netscreen Screenos	6.3.0r9	All	All	All

References

Reference	Source	Lin
2018-10 Security Bulletin: ScreenOS: Stored Cross-Site Scripting (XSS) vulnerability (CVE-2018-0059) - Juniper Networks	CONFIRM	kb.j
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

Vendor Comments And Credit

Discovery Credit

LEGACY: Marcel Bilal from IT-Dienstleistungszentrum Berlin

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](#) 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](#)