



CVE-2017-2338

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

Summary

CVE	CVE-2017-2338
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-17 13:18:00 UTC
Updated	2017-07-22 01:29:00 UTC
Description	A persistent cross site scripting vulnerability in NetScreen WebUI of Juniper Networks Juniper NetScreen Firewall+VPN run

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Screenos	6.3.0	All	All	All
Operating System	Juniper	Screenos	6.3.0	r1	All	All
Operating System	Juniper	Screenos	6.3.0	r10	All	All
Operating System	Juniper	Screenos	6.3.0	r11	All	All
Operating System	Juniper	Screenos	6.3.0	r12	All	All
Operating System	Juniper	Screenos	6.3.0	r13	All	All
Operating System	Juniper	Screenos	6.3.0	r14	All	All
Operating System	Juniper	Screenos	6.3.0	r15	All	All
Operating System	Juniper	Screenos	6.3.0	r16	All	All
Operating System	Juniper	Screenos	6.3.0	r17	All	All
Operating System	Juniper	Screenos	6.3.0	r18	All	All
Operating System	Juniper	Screenos	6.3.0	r19	All	All
Operating System	Juniper	Screenos	6.3.0	r2	All	All
Operating System	Juniper	Screenos	6.3.0	r21	All	All
Operating System	Juniper	Screenos	6.3.0	r22	All	All
Operating System	Juniper	Screenos	6.3.0	r23	All	All
Operating System	Juniper	Screenos	6.3.0	r23b	All	All

Operating System	Juniper	Screenos	6.3.0	r3	All	All
Operating System	Juniper	Screenos	6.3.0	r4	All	All
Operating System	Juniper	Screenos	6.3.0	r5	All	All
Operating System	Juniper	Screenos	6.3.0	r6	All	All
Operating System	Juniper	Screenos	6.3.0	r7	All	All
Operating System	Juniper	Screenos	6.3.0	r8	All	All
Operating System	Juniper	Screenos	6.3.0	r9	All	All
Operating System	Juniper	Screenos	6.3.0	All	All	All
Operating System	Juniper	Screenos	6.3.0	r1	All	All
Operating System	Juniper	Screenos	6.3.0	r10	All	All
Operating System	Juniper	Screenos	6.3.0	r11	All	All
Operating System	Juniper	Screenos	6.3.0	r12	All	All
Operating System	Juniper	Screenos	6.3.0	r13	All	All
Operating System	Juniper	Screenos	6.3.0	r14	All	All
Operating System	Juniper	Screenos	6.3.0	r15	All	All
Operating System	Juniper	Screenos	6.3.0	r16	All	All
Operating System	Juniper	Screenos	6.3.0	r17	All	All
Operating System	Juniper	Screenos	6.3.0	r18	All	All
Operating System	Juniper	Screenos	6.3.0	r19	All	All
Operating System	Juniper	Screenos	6.3.0	r2	All	All
Operating System	Juniper	Screenos	6.3.0	r21	All	All
Operating System	Juniper	Screenos	6.3.0	r22	All	All
Operating System	Juniper	Screenos	6.3.0	r23	All	All
Operating System	Juniper	Screenos	6.3.0	r23b	All	All
Operating System	Juniper	Screenos	6.3.0	r3	All	All
Operating System	Juniper	Screenos	6.3.0	r4	All	All
Operating System	Juniper	Screenos	6.3.0	r5	All	All
Operating System	Juniper	Screenos	6.3.0	r6	All	All
Operating System	Juniper	Screenos	6.3.0	r7	All	All
Operating System	Juniper	Screenos	6.3.0	r8	All	All
Operating System	Juniper	Screenos	6.3.0	r9	All	All

References

Reference	Source	Link
Juniper ScreenOS Input Validation Flaw Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	www.sectrack.com
2017-07-20: Juniper ScreenOS 6.3.0 Multiple XSS Vulnerabilities - CVE-2017-13711, CVE-2017-13712, CVE-2017-13713	CONFIRM	https://www.cve.org/CVER/nid/40102/2017-13711

2017-07 Security Bulletin: ScreenOS: Multiple XSS vulnerabilities in ScreenOS Firewall - Juniper Networks	CONFIRM	kb.juniper.com
Juniper ScreenOS Multiple HTML Injection Vulnerabilities	BID	www.securityfocus.com/bid
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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](#)