



CVE-2018-0014

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

Summary

CVE	CVE-2018-0014
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-10 22:29:00 UTC
Updated	2019-10-09 23:30:00 UTC
Description	Juniper Networks ScreenOS devices do not pad Ethernet packets with zeros, and thus some packets can contain fragment

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Screenos	6.3.0r1	All	All	All
Operating System	Juniper	Screenos	6.3.0r10	All	All	All
Operating System	Juniper	Screenos	6.3.0r11	All	All	All
Operating System	Juniper	Screenos	6.3.0r12	All	All	All
Operating System	Juniper	Screenos	6.3.0r13	All	All	All
Operating System	Juniper	Screenos	6.3.0r14	All	All	All
Operating System	Juniper	Screenos	6.3.0r15	All	All	All
Operating System	Juniper	Screenos	6.3.0r16	All	All	All
Operating System	Juniper	Screenos	6.3.0r17	All	All	All
Operating System	Juniper	Screenos	6.3.0r18	All	All	All
Operating System	Juniper	Screenos	6.3.0r19	All	All	All
Operating System	Juniper	Screenos	6.3.0r2	All	All	All
Operating System	Juniper	Screenos	6.3.0r20	All	All	All
Operating System	Juniper	Screenos	6.3.0r21	All	All	All
Operating System	Juniper	Screenos	6.3.0r22	All	All	All
Operating System	Juniper	Screenos	6.3.0r23	All	All	All
Operating System	Juniper	Screenos	6.3.0r24	All	All	All

Operating System	Juniper	Screenos	6.3.0r25	All	All	All
Operating System	Juniper	Screenos	6.3.0r3	All	All	All
Operating System	Juniper	Screenos	6.3.0r4	All	All	All
Operating System	Juniper	Screenos	6.3.0r5	All	All	All
Operating System	Juniper	Screenos	6.3.0r6	All	All	All
Operating System	Juniper	Screenos	6.3.0r7	All	All	All
Operating System	Juniper	Screenos	6.3.0r8	All	All	All
Operating System	Juniper	Screenos	6.3.0r9	All	All	All
Operating System	Juniper	Screenos	6.3.0r1	All	All	All
Operating System	Juniper	Screenos	6.3.0r10	All	All	All
Operating System	Juniper	Screenos	6.3.0r11	All	All	All
Operating System	Juniper	Screenos	6.3.0r12	All	All	All
Operating System	Juniper	Screenos	6.3.0r13	All	All	All
Operating System	Juniper	Screenos	6.3.0r14	All	All	All
Operating System	Juniper	Screenos	6.3.0r15	All	All	All
Operating System	Juniper	Screenos	6.3.0r16	All	All	All
Operating System	Juniper	Screenos	6.3.0r17	All	All	All
Operating System	Juniper	Screenos	6.3.0r18	All	All	All
Operating System	Juniper	Screenos	6.3.0r19	All	All	All
Operating System	Juniper	Screenos	6.3.0r2	All	All	All
Operating System	Juniper	Screenos	6.3.0r20	All	All	All
Operating System	Juniper	Screenos	6.3.0r21	All	All	All
Operating System	Juniper	Screenos	6.3.0r22	All	All	All
Operating System	Juniper	Screenos	6.3.0r23	All	All	All
Operating System	Juniper	Screenos	6.3.0r24	All	All	All
Operating System	Juniper	Screenos	6.3.0r25	All	All	All
Operating System	Juniper	Screenos	6.3.0r3	All	All	All
Operating System	Juniper	Screenos	6.3.0r4	All	All	All
Operating System	Juniper	Screenos	6.3.0r5	All	All	All
Operating System	Juniper	Screenos	6.3.0r6	All	All	All
Operating System	Juniper	Screenos	6.3.0r7	All	All	All
Operating System	Juniper	Screenos	6.3.0r8	All	All	All
Operating System	Juniper	Screenos	6.3.0r9	All	All	All

References

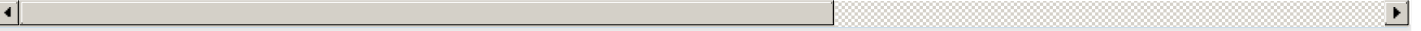
Reference

2018-01 Security Bulletin: ScreenOS: Etherleak vulnerability found on ScreenOS device (CVE-2018-0014) - Juniper Networks

Juniper ScreenOS Etherleak Flaw Lets Remote Users Obtain Potentially Sensitive Information from Unpadded Ethernet Packets - SecurityTra

CVE Program record

NVD vulnerability detail



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](#)