



CVE-2015-7754

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-7754
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-08 19:59:00 UTC
Updated	2016-01-13 18:55:00 UTC
Description	Juniper ScreenOS before 6.3.0r21, when ssh-pka is configured and enabled, allows remote attackers to cause a denial of s

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Screenos	All	r20	All	All

References

Reference

- Juniper ScreenOS CVE-2015-7754 Denial of Service Vulnerability
- Juniper ScreenOS Bug in ssh-pka Lets Remote Users Deny Service or Execute Arbitrary Code on the Target System - SecurityTracker
- Juniper Networks - 2015-12 Out of Cycle Security Bulletin: ScreenOS: Crafted SSH negotiation may trigger system crash (CVE-2015-7754) - I
- 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.

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