



# CVE-2002-2150

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

## Summary

<b>CVE</b>	CVE-2002-2150
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2002-12-31 05:00:00 UTC
<b>Updated</b>	2008-09-05 20:32:00 UTC
<b>Description</b>	Firewalls from multiple vendors empty state tables more slowly than they are filled, which allows remote attackers to flood s

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.10_r3	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.10_r4	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.7.1	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.7.1r1	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.7.1r2	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.7.1r3	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	3.0.1r1	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	3.0.1r2	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	3.0.3_r1.1	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.10_r3	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.10_r4	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.7.1	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.7.1r1	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.7.1r2	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	2.7.1r3	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	3.0.1r1	All	All	All
Operating System	<a href="#">Juniper</a>	<a href="#">Netscreen Screenos</a>	3.0.1r2	All	All	All

Operating System	Juniper	Netscreen Screenos	3.0.3_r1.1	All	All	All
------------------	---------	--------------------	------------	-----	-----	-----

## References

Reference	Source	Link
ISS X-Force Database: firewall-state-table-dos (10449): Multiple firewall full state table denial of service	XF	<a href="http://www.iss.net">www.iss.net</a>
CERT/CC Vulnerability Note VU#539363	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>
Multiple Firewall Vendor Packet Flood State Table Filling Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)