



# CVE-2008-1397

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

## Summary

<b>CVE</b>	CVE-2008-1397
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-03-20 00:44:00 UTC
<b>Updated</b>	2017-08-08 01:30:00 UTC
<b>Description</b>	Check Point VPN-1 Power/UTM, with NGX R60 through R65 and NG AI R55 software, allows remote authenticated users to

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Checkpoint</a>	<a href="#">Check Point Vpn-1 Pro</a>	ngx_r61	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Check Point Vpn-1 Pro</a>	ngx_r62_ga	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Check Point Vpn-1 Pro</a>	ngx_r61	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Check Point Vpn-1 Pro</a>	ngx_r62_ga	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Vpn-1</a>	ngx_r60	All	pro	All
Application	<a href="#">Checkpoint</a>	<a href="#">Vpn-1</a>	ngx_r60	All	pro	All
Application	<a href="#">Checkpoint</a>	<a href="#">Vpn-1 Firewall-1</a>	ng_ai_r55	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Vpn-1 Firewall-1</a>	ng_ai_r55	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Vpn-1 Power Utm</a>	ngx_r65_with_messaging_security	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Vpn-1 Power Utm</a>	ngx_r65_with_messaging_security	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Vpn-1 Power Utm With Ngx</a>	r65	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Vpn-1 Power Utm With Ngx</a>	r65	All	All	All

## References

Reference	Source	Link
Pure Security	MISC	<a href="#">purese</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.v</a>

CheckPoint VPN-1 IP Address Collision Security Issue - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="#">secunia.com</a>
IBM X-Force Exchange	XF	<a href="#">exchange.ibm.com</a>
Support, Support Requests, Training, Documentation, and Knowledge base for Check Point products and services	CONFIRM	<a href="#">support.checkpoint.com</a>
<a href="#">www.puresecurity.com.au/files/PureSecurity%20VPN-1%20DoS_Spoofing%20Attack%20against%20...</a>	MISC	<a href="#">www.puresecurity.com.au</a>
US-CERT Vulnerability Notes	CERT-VN	<a href="#">www.kirtland.gov/cert/vn</a>
Check Point VPN-1 IP Address Collision Denial of Service Vulnerability	BID	<a href="#">www.bids.cve.org</a>
Check Point VPN-1 SecuRemote Lets Remote Users Deny Service - SecurityTracker	SECTRACK	<a href="#">www.securitytracker.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">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](#) 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](#)