



CVE-2005-2889

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

Summary

CVE	CVE-2005-2889
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-09-14 20:03:00 UTC
Updated	2016-10-18 03:31:00 UTC
Description	Check Point NGX R60 does not properly verify packets against the predefined service group "CIFS" rule, which allows remote users to bypass the rule and access the system.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkpoint	Connectra Ngx	r60	All	All	All
Application	Checkpoint	Connectra Ngx	r60	All	All	All

References

Reference	Source	Link	Tags
'Rule bypassing in CheckPoint NGX R60' - MARC	BUGTRAQ	marc.info	
US-CERT Vulnerability Note VU#508209	CERT-VN	www.kb.cert.org	US Government Resource
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#)