CVE-2010-3010

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2010-3010
State	PUBLISHED
Assigner	hp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-09-15 20:00:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability on the HP 3Com OfficeConnect Gigabit VPN Firewall 3CREVF100-73 with firmware

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	3com Officeconnect Gigabit Vpn Firewall Software	1.0.8	All	All	All

Operating System	Hp	3com Officeconnect Gigabit Vpn Firewall Software	All	All	All	All
Hardware	Hp	3crevf100-73	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Sourc
h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp	af854
SecurityTracker.com Archives - 3Com OfficeConnect Gigabit VPN Firewall Input Validation Hole Permits Cross-Site Scripting Attacks	af854
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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