CVE-2008-2637

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

Summary

CVE	CVE-2008-2637
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-10 00:32:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in F5 FirePass SSL VPN 6.0.2 hotfix 3, and possibly earlier versions, allow

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
Application	F5	Firepass Ssl Vpn	6.0.2	hotfix_3	All	All

Vendor Declared Affected Products

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

References

Reference
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
SecurityTracker.com Archives - F5 FirePass Input Validation Hole in 'css_exceptions' and 'sql_matchscope' Parameters Permits Cross-Site Sc
SecurityFocus
IBM X-Force Exchange
SecurityReason - F5 FirePass Content Inspection Management XSS
F5 FirePass SSL VPN Appliance Cross-Site Scripting Vulnerabilities - Advisories - Secunia
F5 FirePass SSL VPN Multiple Cross-Site Request Forgery Vulnerabilities
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.