CVE-2004-0039

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

Summary

CVE	CVE-2004-0039
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-03-03 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple format string vulnerabilities in HTTP Application Intelligence (AI) component in Check Point Firewall-1 NG-AI R55 a

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkpoint	Firewall-1	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
O-072: Check Point FireWall-1 HTTP Security Server Vulnerability	af854a3a-2127-422b-91ae-3
xforce.iss.net/xforce/alerts/id/162	af854a3a-2127-422b-91ae-3
US-CERT Technical Cyber Security Alert TA04-036A -- HTTP Parsing Vulnerabilities in Check Point Firewall-1	af854a3a-2127-422b-91ae-3
US-CERT Vulnerability Note VU#790771	af854a3a-2127-422b-91ae-3
Multiple Check Point Firewall-1 HTTP Security Server Remote Format String Vulnerabilities	af854a3a-2127-422b-91ae-3
Check Point Software: FireWall-1 HTTP Security Server Vulnerability	af854a3a-2127-422b-91ae-3
marc.info	af854a3a-2127-422b-91ae-3
IBM X-Force Exchange	af854a3a-2127-422b-91ae-3
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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