CVE-2007-2688

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

Summary

CVE	CVE-2007-2688
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-16 01:19:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The Cisco Intrusion Prevention System (IPS) and IOS with Firewall/IPS Feature Set do not properly handle certain full-width

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios	10.0	All	All	All

Operating System	Cisco	Ios	11.1cc	All	All	All
Operating System	Cisco	Ios	11.3	All	All	All
Operating System	Cisco	Ios	12.0	All	All	All
Operating System	Cisco	Ios	12.0s	All	All	All
Operating System	Cisco	Ios	12.0st	All	All	All
Operating System	Cisco	Ios	12.0t	All	All	All
Operating System	Cisco	Ios	12.1	All	All	All
Operating System	Cisco	Ios	12.1e	All	All	All
Operating System	Cisco	Ios	12.1t	All	All	All
Operating System	Cisco	Ios	12.2	All	All	All
Operating System	Cisco	Ios	12.2t	All	All	All
Application	Cisco	Ips Sensor Software	4.0	All	All	All
Application	Cisco	Ips Sensor Software	5.0\(1\)	All	All	All
Application	Cisco	Ips Sensor Software	5.0\(2\)	All	All	All
Application	Cisco	Ips Sensor Software	5.0\(6\)p1	All	All	All
Application	Cisco	Ips Sensor Software	5.1\(1a\)	All	All	All
Application	Cisco	Ips Sensor Software	5.1\(1b\)	All	All	All
Application	Cisco	Ips Sensor Software	5.1\(1c\)	All	All	All
Application	Cisco	Ips Sensor Software	5.1\(1d\)	All	All	All
Application	Cisco	Ips Sensor Software	5.1\(1e\)	All	All	All
Application	Cisco	Ips Sensor Software	5.1\(1\)	All	All	All
Application	Cisco	Ips Sensor Software	5.1\(p1\)	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
IBM X-Force Exchange	af854a3a-21
Cisco Intrusion Prevention System Lets Remote Users Evade Detection With Certain Character Encodings - SecurityTracker	af854a3a-21
US-CERT Vulnerability Note VU#739224	af854a3a-21
www.gamasec.net/english/gs07-01.html	af854a3a-21
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-21
Cisco Products HTTP Unicode Encoding Detection Bypass - Advisories - Secunia	af854a3a-21
Multiple Products Full/Half Width Unicode Detection Evasion Vulnerability	af854a3a-21
Repository / Oval Repository	af854a3a-21

Repository / Oval Repository	af854a3a-21
Cisco Security Response: HTTP Full-Width and Half-Width Unicode Encoding Evasion [Products & Services] - Cisco Systems	af854a3a-21
www.osvdb.org/35336	af854a3a-21
SecurityFocus	af854a3a-21
Cisco IOS Firewall/IPS Feature Set Lets Remote Users Evade Detection With Certain Character Encodings - SecurityTracker	af854a3a-21
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**