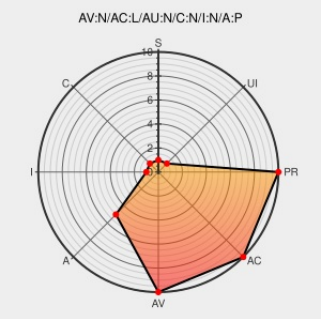
CVE-2011-4022

Published on: 05/03/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:10 PM UTC

CVE-2011-4022

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Intrusion Prevention System from Cisco contain the following vulnerability:

The sensor in Cisco Intrusion Prevention System (IPS) 7.0 and 7.1 allows remote attackers to cause a denial of service (file-handle exhaustion and mainApp hang) by making authentication attempts that exceed the configured limit, aka Bug ID CSCto51204.

CVE-2011-4022 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
	www.cisco.com text/plain	CONFIRM www.cisco.com/web/software/282549709/56954/IPS-7-1-3-E4_readme.txt

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Cisco	Intrusion Prevention System	7.0	All	All	All
Application	Cisco	Intrusion Prevention System	7.1	All	All	All
Application	Cisco	Intrusion Prevention System	7.0	All	All	All
Application	Cisco	Intrusion Prevention System	7.1	All	All	All

cpe:2.3:a:cisco:intrusion_prevention_system:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:intrusion_prevention_system:7.1:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:intrusion_prevention_system:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:intrusion_prevention_system:7.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→