CVE-2013-3445

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

Summary

CVE	CVE-2013-3445
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-29 13:59:06 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The firewall subsystem in Cisco Identity Services Engine has an incorrect rule for open ports, which allows remote attackers

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Identity Services Engine	-	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Cisco Identity Services Engine High CPU Utilization Vulnerability	af854a3a-2127-422b-91
Cisco Identity Services Engine Software CVE-2013-3445 Denial of Service Vulnerability	af854a3a-2127-422b-91
Cisco Identity Services Engine High CPU Utilization Vulnerability	af854a3a-2127-422b-91
Cisco Identity Services Engine Flaw in Firewall Implementation Lets Remote Users Deny Service - SecurityTracker	af854a3a-2127-422b-91
osvdb.org/95659	af854a3a-2127-422b-91
IBM X-Force Exchange	af854a3a-2127-422b-91
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.