CVE-2001-0375

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

Summary

CVE	CVE-2001-0375
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-06-18 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Cisco PIX Firewall 515 and 520 with 5.1.4 OS running aaa authentication to a TACACS+ server allows remote attackers to

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: NVD-CWE-Other | 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	Pix Firewall 515	All	All	All	All

Hardware	Cisco	Pix Firewall 520	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	Link
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.co
Cisco PIX Firewall Authentication Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.cisco.com
'PIX Firewall 5.1 DoS Vulnerability' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
Cisco PIX TACACS+ Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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