CVE-2000-0613

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

Summary

CVE	CVE-2000-0613
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2000-03-20 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Cisco Secure PIX Firewall does not properly identify forged TCP Reset (RST) packets, which allows remote attackers to for

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
Application	Cisco	Pix Firewall	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	T
www.osvdb.org/1457	af854a3a-2127-422b-91ae-364da2661108	www.osvdb.org	
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.com	
Cisco - Cisco Secure PIX Firewall TCP Reset Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.cisco.com	
Cisco Secure PIX Firewall Forged TCP RST Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	
SecurityFocus	MITRE	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

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