CVE-2009-1160

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

Summary

CVE	CVE-2009-1160
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-09 15:08:00 UTC
Updated	2009-04-28 05:39:00 UTC
Description	Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.0 before 7.0(8)1, 7.1 before 7.1(2)74

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Adaptive Security Appliance 5500	7.0	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	7.1	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	7.2	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	8.0	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	8.1	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	7.0	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	7.1	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	7.2	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	8.0	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	8.1	All	All	All
Hardware	Cisco	Pix	7.0	All	All	All
Hardware	Cisco	Pix	7.1	All	All	All
Hardware	Cisco	Pix	7.2	All	All	All
Hardware	Cisco	Pix	8.0	All	All	All
Hardware	Cisco	Pix	7.0	All	All	All
Hardware	Cisco	Pix	7.1	All	All	All
Hardware	Cisco	Pix	7.2	All	All	All

Hardware	Cisco	Pix	8.0	All	All	All

References

Reference
Cisco PIX and ASA Multiple Denial of Service, ACL Bypass, and Authentication Bypass Vulnerabilities
Cisco Security Advisory: Multiple Vulnerabilities in Cisco ASA Adaptive Security Appliance and Cisco PIX Security Appliances [Products & Se
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Cisco ASA and PIX Multiple Vulnerabilities - Advisories - Community
Cisco ASA Bug Lets Remote Users Bypass Access Control List Implicit Deny Feature - SecurityTracker
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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