CVE-2006-0181

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

Summary

CVE	CVE-2006-0181
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-01-12 06:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Cisco Security Monitoring, Analysis and Response System (CS-MARS) before 4.1.3 has an undocumented administrative a

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Cs-mars	4.1	All	All	All

Hardware	Cisco	Cs-mars	4.1.2	All	All	All

Vendor Declared Affected Products

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

References

Reference
SecurityTracker.com Archives - Cisco Security Monitoring, Analysis and Response System (CS-MARS) Undocumented Account With Default
www.osvdb.org/22346
Bugtraq: Cisco, haven't we learned anything? (technician reset)
Default Administrative Password in Cisco Security Monitoring, Analysis and Response System (CS-MARS) - SecurityReason.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Cisco CS-MARS Undocumented Root Account Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Cisco CS-MARS Default Administrative Password Vulnerability
Cisco - Networking, Cloud, and Cybersecurity Solutions
IBM X-Force Exchange
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.