CVE-2008-2234

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

Summary

CVE	CVE-2008-2234
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-18 17:41:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Multiple buffer overflows in Openwsman 1.2.0 and 2.0.0 allow remote attackers to execute arbitrary code via a crafted "Auth

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openwsman	Openwsman	1.2.0	All	All	All

Application	Openwsman	Openwsman	2.0.0	All	All	All

Vendor Declared Affected Products

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

References

Reference
openwsman HTTP Basic Authentication Buffer Overflow - Secunia Advisories - Vulnerability Information - Secunia.com
SUSE update for openwsman - Secunia.com
SecurityFocus
VMware ESX / ESXi openwsman HTTP Basic Authentication Buffer Overflow - Secunia Advisories - Vulnerability Intelligence - Secunia.com
IBM X-Force Exchange
IBM X-Force Exchange
[security-announce] SUSE Security Announcement: openwsman (SUSE-SA:2008:
VMSA-0008-0015 - VMware
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Openwsman Multiple Remote Security Vulnerabilities
[Security-announce] VMSA-2008-0015 Updated ESXi and ESX 3.5 packages address critical security issue in openwsman
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
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.