CVE-2012-6530

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

Summary

CVE	CVE-2012-6530
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-01-31 05:44:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Stack-based buffer overflow in Sysax Multi Server before 5.52, when HTTP is enabled, allows remote authenticated users v

Risk And Classification

Primary CVSS: v2.0 7.1 from nvd@nist.gov

AV:N/AC:H/Au:S/C:C/I:C/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:H/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sysax	Multi Server	4.3	All	All	All

Application	Sysax	Multi Server	4.5	All	All	All
Application	Sysax	Multi Server	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
pwnag3: Sysax Multi Server 5.50 Exploit	af854a3a-2127-422b-91ae-364da2661108	www.pwnag3.c
Sysax Multi Server 5.50 Create Folder BOF	af854a3a-2127-422b-91ae-364da2661108	www.exploit-db
Sysax Multi Server 'Content-Disposition' Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfo
Sysax Multi Server 5.50 Create Folder Remote Code Exec BoF (MSF Module)	af854a3a-2127-422b-91ae-364da2661108	www.exploit-db
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.