CVE-2011-4189

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

Summary

CVE	CVE-2011-4189
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-03-02 22:55:00 UTC
Updated	2018-01-11 02:29:00 UTC
Description	The client in Novell GroupWise 8.0x through 8.02HP3 allows remote attackers to execute arbitrary code or cause a denial c

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Novell	Groupwise	8.0	All	All	All
Application	Novell	Groupwise	8.0	hp1	All	All
Application	Novell	Groupwise	8.0	hp2	All	All
Application	Novell	Groupwise	8.0	sp1	All	All
Application	Novell	Groupwise	8.0.1	All	All	All
Application	Novell	Groupwise	8.0.2	All	All	All
Application	Novell	Groupwise	8.0.2	hp1	All	All
Application	Novell	Groupwise	8.0	All	All	All
Application	Novell	Groupwise	8.0	hp1	All	All
Application	Novell	Groupwise	8.0	hp2	All	All
Application	Novell	Groupwise	8.0	sp1	All	All
Application	Novell	Groupwise	8.0.1	All	All	All
Application	Novell	Groupwise	8.0.2	All	All	All
Application	Novell	Groupwise	8.0.2	hp1	All	All

References

Reference	Source	Link

IBM X-Force Exchange	XF	excl
79720	OSVDB	osv
Novell GroupWise Client Address Book Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	ww
Access Denied	CONFIRM	bug
Security Advisory SA48199 - Novell GroupWise Client Address Book Processing Buffer Overflow Vulnerability - Secunia	SECUNIA	sec
Support | Security Vulnerability - GroupWise 8 Windows Client Address Book Remote Code Execution Vulnerability	CONFIRM	ww
Novell Groupwise Client CVE-2011-4189 Address Book Parsing Remote Code Execution Vulnerability	BID	ww
{PRL} Novell Groupwise Address Book Remote Code Execution	MISC	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**