



CVE-2009-1635

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2009-1635
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-05-22 16:48:00 UTC
Updated	2018-10-10 19:37:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the WebAccess component in Novell GroupWise 7.x before 7.03 HP3 and

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Novell	Groupwise	7.0	All	All	All
Application	Novell	Groupwise	7.0	sp1	All	All
Application	Novell	Groupwise	7.0	sp2	All	All
Application	Novell	Groupwise	7.0	sp3	All	All
Application	Novell	Groupwise	7.0.0	sp1	All	All
Application	Novell	Groupwise	7.0.0	sp2	All	All
Application	Novell	Groupwise	7.0.2	All	All	All
Application	Novell	Groupwise	7.0.3	All	All	All
Application	Novell	Groupwise	7.01	All	All	All
Application	Novell	Groupwise	7.02x	All	All	All
Application	Novell	Groupwise	7.03	All	All	All
Application	Novell	Groupwise	7.03	hp1a	All	All
Application	Novell	Groupwise	7.03	hp2	All	All
Application	Novell	Groupwise	8.0	All	All	All
Application	Novell	Groupwise	8.0	hp1	All	All
Application	Novell	Groupwise	7.0	All	All	All
Application	Novell	Groupwise	7.0	sp1	All	All

Application	Novell	Groupwise	7.0	sp2	All	All
Application	Novell	Groupwise	7.0	sp3	All	All
Application	Novell	Groupwise	7.0.0	sp1	All	All
Application	Novell	Groupwise	7.0.0	sp2	All	All
Application	Novell	Groupwise	7.0.2	All	All	All
Application	Novell	Groupwise	7.0.3	All	All	All
Application	Novell	Groupwise	7.01	All	All	All
Application	Novell	Groupwise	7.02x	All	All	All
Application	Novell	Groupwise	7.03	All	All	All
Application	Novell	Groupwise	7.03	hp1a	All	All
Application	Novell	Groupwise	7.03	hp2	All	All
Application	Novell	Groupwise	8.0	All	All	All
Application	Novell	Groupwise	8.0	hp1	All	All

References			
Reference	Source	Link	
Novell GroupWise WebAccess - Security Vulnerability with Javascript	CONFIRM	wv	
IBM X-Force Exchange	XF	ex	
Access Denied	MISC	bu	
Novell GroupWise WebAccess 'gw/webacc' Multiple Cross-Site Scripting Vulnerabilities	BID	wv	
IBM X-Force Exchange	XF	ex	
SecurityFocus	BUGTRAQ	wv	
Novell GroupWise Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	se	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	wv	
packetstorm.linuxsecurity.com/0905-exploits/groupwise-xss.txt	MISC	pa	
Novell GroupWise WebAccess - Scripting Security Vulnerability	CONFIRM	wv	
Novell GroupWise WebAccess - Cross Site Scripting (XSS) Security Vulnerability via Unfiltered Style Expressions	CONFIRM	wv	
SecurityFocus	BUGTRAQ	wv	
IBM X-Force Exchange	XF	ex	
Access Denied	MISC	bu	
Access Denied	MISC	bu	
Novell GroupWise WebAccess Multiple Security Vulnerabilities	BID	wv	
Novell GroupWise WebAccess Input Validation Flaw in Login Page Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRAK	se	
CVE Program record	CVE.ORG	wv	
NVD vulnerability detail	NVD	nv	

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)