



CVE-2007-6435

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

Summary

CVE	CVE-2007-6435
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-18 20:46:00 UTC
Updated	2018-10-15 21:54:00 UTC
Description	Stack-based buffer overflow in Novell GroupWise before 6.5.7, when HTML preview of e-mail is enabled, allows user-assist

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Novell	Groupwise	All	All	All	All

References

Reference
ISR, Infobyte Security Research
IBM X-Force Exchange
SecurityTracker.com Archives - Novell GroupWise Stack Overflow in Processing IMG SRC Tag Lets Remote Users Execute Arbitrary Code
Novell GroupWise Client HTML E-Mail Processing Buffer Overflow - Advisories - Secunia
Novell GroupWise 'img' Tag Buffer Overflow Vulnerability
40870
Webmail - OVH
SecurityFocus
SecurityReason - Novell Groupwise client remote stack overflow silently patched.
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.

© [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](#)