



CVE-2007-4474

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

Summary

CVE	CVE-2007-4474
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-27 22:46:00 UTC
Updated	2017-09-29 01:29:00 UTC
Description	Multiple stack-based buffer overflows in the IBM Lotus Domino Web Access ActiveX control, as provided by inotes6.dll, inot

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Domino Web Access	6.0	All	All	All
Application	ibm	Domino Web Access	6.0.1	All	All	All
Application	ibm	Domino Web Access	6.0.1.1	All	All	All
Application	ibm	Domino Web Access	6.0.2	All	All	All
Application	ibm	Domino Web Access	6.0.3	All	All	All
Application	ibm	Domino Web Access	6.0.4	All	All	All
Application	ibm	Domino Web Access	6.0.5	All	All	All
Application	ibm	Domino Web Access	6.5	All	All	All
Application	ibm	Domino Web Access	6.5.1	All	All	All
Application	ibm	Domino Web Access	6.5.2	All	All	All
Application	ibm	Domino Web Access	6.5.3	All	All	All
Application	ibm	Domino Web Access	6.5.4	All	All	All
Application	ibm	Domino Web Access	6.5.5	All	All	All
Application	ibm	Domino Web Access	7.0	All	All	All
Application	ibm	Domino Web Access	7.0.1	All	All	All
Application	ibm	Domino Web Access	6.0	All	All	All
Application	ibm	Domino Web Access	6.0.1	All	All	All

Application	ibm	Domino Web Access	6.0.1.1	All	All	All
Application	ibm	Domino Web Access	6.0.2	All	All	All
Application	ibm	Domino Web Access	6.0.3	All	All	All
Application	ibm	Domino Web Access	6.0.4	All	All	All
Application	ibm	Domino Web Access	6.0.5	All	All	All
Application	ibm	Domino Web Access	6.5	All	All	All
Application	ibm	Domino Web Access	6.5.1	All	All	All
Application	ibm	Domino Web Access	6.5.2	All	All	All
Application	ibm	Domino Web Access	6.5.3	All	All	All
Application	ibm	Domino Web Access	6.5.4	All	All	All
Application	ibm	Domino Web Access	6.5.5	All	All	All
Application	ibm	Domino Web Access	7.0	All	All	All
Application	ibm	Domino Web Access	7.0.1	All	All	All
Application	ibm	Lotus Domino Web Access	7.0.1	All	All	All
Application	ibm	Lotus Domino Web Access	7.0.34.1	All	All	All
Application	ibm	Lotus Domino Web Access	7.0.1	All	All	All
Application	ibm	Lotus Domino Web Access	7.0.34.1	All	All	All

References

Reference

[Full-disclosure] IBM Domino Web Access Upload Control dwa7w.dll Memory Corruption

IBM X-Force Exchange

SecurityTracker.com Archives - IBM Domino Web Access 'dwa7w.dll' ActiveX Control Buffer Overflow May Let Remote Users Execute Arbitra

IBM Lotus Domino Web Access Control ActiveX Control Buffer Overflow - Advisories - Secunia

IBM Domino Web Access Upload Module inotes6.dll BoF Exploit

IBM Domino Web Access Upload Module SEH Overwrite Exploit

40954

IBM Domino Web Access Upload Module dwa7w.dll BoF Exploit

VU#963889 - IBM Lotus Domino Web Access ActiveX control stack buffer overflows

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

IBM Lotus Domino Web Access ActiveX Control Memory Corruption Vulnerabilities

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](#)