



CVE-2009-4654

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

Summary

CVE	CVE-2009-4654
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-02-26 18:30:00 UTC
Updated	2018-10-10 19:49:00 UTC
Description	Stack-based buffer overflow in the dhost module in Novell eDirectory 8.8 SP5 for Windows allows remote authenticated users to execute arbitrary code via a crafted HTTP request.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Application	Novell	Edirectory	8.8	sp5	All	All
Application	Novell	Edirectory	8.8	sp5	All	All

References

Reference
IBM X-Force Exchange
SecurityFocus
SecurityTracker.com Archives - Novell eDirectory Buffer Overflow in HTTPSTK Login Page Lets Remote Authenticated Users Execute Arbitrary Code
tcc.hellcode.net/sploit/htpstkt.txt
downloads.securityfocus.com/vulnerabilities/exploits/37042-2.pl
tcc.hellcode.net/advisories/hellcode-adv005.txt
Novell eDirectory 'dhost/httpstk' Multiple Stack Buffer Overflow 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](#)