

[NEWS] Novell eDirectory for Linux Stack Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00076.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 31 Mar 2008 15:15:09 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Novell eDirectory for Linux Stack Overflow

SUMMARY

<<http://www.novell.com/products/edirectory/>> Novell eDirectory is "the foundation for the world's largest identity management deployments. With eDirectory, businesses lay the groundwork for secure identity management solutions and multi-platform network services". A vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Novell eDirectory for Linux. Authentication is not required to exploit this vulnerability.

DETAILS

Vulnerable Systems:

- * Novell eDirectory version 8.8.1
- * Novell eDirectory version 8.7.3.9 (8.7.3 SP9)

Immune Systems:

- * Novell eDirectory version 8.8.2
- * Novell eDirectory version 8.7.3.10 (8.7.3 SP10)

The specific flaw exists in the libndap library. When a large LDAP delRequest message is sent, a stack overflow occurs overwriting a function

[NEWS] Novell eDirectory for Linux Stack Overflow

pointer. This results in a situation allowing the execution of arbitrary code.

Vendor Response:

Novell has issued an update to correct this vulnerability. More details can be found at:

http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3382120&sliceId=SAL_Public
http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3382120&sliceId=SAL_Public

Disclosure Timeline:

2007-07-20 – Vulnerability reported to vendor
2008-03-26 – Coordinated public release of advisory

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0924>
CVE-2008-0924

ADDITIONAL INFORMATION

The information has been provided by zdi-disclosures@xxxxxxxxx
The Zero Day Initiative (ZDI).

The original article can be found at:
<http://www.zerodayinitiative.com/advisories/ZDI-08-013>
<http://www.zerodayinitiative.com/advisories/ZDI-08-013>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.