

[UNIX] Novell SUSE Linux Enterprise Server Remote Manager Heap Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00043.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Jan 2006 19:06:28 +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 SUSE Linux Enterprise Server Remote Manager Heap Overflow

SUMMARY

Novell Open Enterprise Server is "a secure, highly available suite of services that provides proven networking, communication, collaboration and application services in an open, easy-to-deploy environment".

Improper input validation allows attackers to cause a buffer overflow and execute arbitrary code on Novell SuSE Linux.

DETAILS

Vulnerable Systems:

- * Novell SUSE Linux Enterprise Server 9

The vulnerability specifically exists due to improper handling of a an HTTP POST request with a negative Content-Length parameter. When such a request is received, controllable heap corruption occurs which can lead to the execution of arbitrary code using traditional Linux heap overflow methods. The following HTTP request can be used to trigger this vulnerability.

[UNIX] Novell SUSE Linux Enterprise Server Remote Manager Heap Overflow

POST / HTTP/1.0
Content-Length: -900

DATA_THAT_WILL_BE_USED_TO_OVERWRITE_THE_HEAP

With careful manipulation of the string, an arbitrary 4 byte write may be achieved which can be used to gain execution control and execute arbitrary code.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3655>>
CVE-2005-3655

Disclosure Timeline:

11/15/2005 – Initial vendor notification
11/15/2005 – Initial vendor response
01/13/2006 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:idlabs-advisories@xxxxxxxxxxxxxxxxxxxxx>> iDEFENSE Labs .

The original article can be found at:
<<http://www.idefense.com/application/poi/display?type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?type=vulnerabilities>

=====

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.

-
- Prev by Date: [*\[EXPL\] Linux Kernel Socket Buffer Memory Exhaustion DoS \(Exploit\)*](#)
 - Next by Date: [*\[NT\] Cisco Security Agent Vulnerable to Crafted IP Attack*](#)
 - Previous by thread: [*\[EXPL\] Linux Kernel Socket Buffer Memory Exhaustion DoS \(Exploit\)*](#)

[UNIX] Novell SUSE Linux Enterprise Server Remote Manager Heap Overflow

- Next by thread: [*\[NT\] Cisco Security Agent Vulnerable to Crafted IP Attack*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)