

[UNIX] Ethereal OSPF Protocol Dissector Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00030.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 11 Dec 2005 11:47:30 +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>

Ethereal OSPF Protocol Dissector Buffer Overflow

SUMMARY

" <<http://www.ethereal.com/>> Ethereal is used by network professionals around the world for troubleshooting, analysis, software and protocol development, and education."

"

<http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=2817&type=ftp&file_format=txt> Open Shortest Path First (OSPF) TCP/IP internet routing protocol is classified as an Interior Gateway Protocol (IGP). This means that it distributes routing information between routers belonging to a single Autonomous System."

Lack of proper length validation of Ethereal OSPF Protocol Dissector allow attackers to execute arbitrary code using a buffer overflow.

DETAILS

Vulnerable Systems:

- * Ethereal version 0.10.0 and above
- * Ethereal version 0.10.12 and prior

[UNIX] Ethereal OSPF Protocol Dissector Buffer Overflow

Immune Systems:

* Ethereal version 0.10.13

The affected Ethereal component is used to analyse Open Shortest Path First (OSPF) Interior Gateway Protocol (IGP), as specified in RFC-2178.

The vulnerability specifically exists due to no bounds checking being performed in the `dissect_ospf_v3_address_prefix()` function. This function takes user-supplied binary data and attempts to convert it into a human readable string. This function uses a fixed length buffer on the stack to store the constructed string but performs no checks on the length of the input. If the generated output length from the input exceeds the size of the buffer, a stack-based overflow occurs.

Successful exploitation allow remote attackers to perform a DoS against a running instance of Ethereal and may, under certain conditions, potentially allow the execution of arbitrary code. As the overflow string is generated from a format string converting binary values into their hexadecimal (base 16) equivalent characters, it can contain only a limited subset of all possible characters, and the length of an overflow is only able to be controlled to within the three characters.

This may prevent exploit ability on some platforms; however, it may be possible that these constraints will not prevent exploitation on others.

Vendor Status:

The vendor has issued a fix for the problem:

<http://anonsvn.ethereal.com/viewcvs/viewcvs.py/trunk/epan/dissectors/packet-ospf.c?rev=16507&view=markup>
<http://anonsvn.ethereal.com/viewcvs/viewcvs.py/trunk/epan/dissectors/packet-ospf.c?rev=16507&view=markup>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3651>
CVE-2005-3651

Disclosure Timeline:

11/14/2005 Initial vendor notification

11/14/2005 Initial vendor response

12/09/2005 Public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<mailto:idlabs-advisories@xxxxxxxxxxxxxxxxxxxxx> iDefense.

The original article can be found at:

<http://www.iddefense.com/application/poi/display?id=349&type=vulnerabilities&flashstatus=true>
<http://www.iddefense.com/application/poi/display?id=349&type=vulnerabilities&flashstatus=true>

=====

[UNIX] Ethereal OSPF Protocol Dissector Buffer Overflow

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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: [*\[NT\] Ipswitch Multiple Vulnerabilities \(IMail IMAP LIST Command DoS, Collaboration Suite SMTP Format String\)*](#)
 - Next by Date: [*\[NEWS\] GTK+ gdk-pixbuf XPM Loader Heap Overflow*](#)
 - Previous by thread: [*\[NT\] Ipswitch Multiple Vulnerabilities \(IMail IMAP LIST Command DoS, Collaboration Suite SMTP Format String\)*](#)
 - Next by thread: [*\[NEWS\] GTK+ gdk-pixbuf XPM Loader Heap Overflow*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)