

[VulnWatch] iDefense Security Advisory 12.09.05: Ethereal OSPF Protocol Dissector Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-12/msg00007.html>

- *From:* "labs-no-reply@xxxxxxxxxxxx" <labs-no-reply@xxxxxxxxxxxx>
 - *Date:* Fri, 09 Dec 2005 16:32:51 -0500
-

Ethereal OSPF Protocol Dissector Buffer Overflow Vulnerability

iDefense Security Advisory 12.09.05
www.idefense.com/application/poi/display?id=349&type=vulnerabilities
December 9, 2005

I. BACKGROUND

Ethereal is a full featured open source network protocol analyzer.

For more information, see <http://www.ethereal.com/>

II. DESCRIPTION

Remote exploitation of an input validation vulnerability in the OSPF protocol dissectors within Ethereal, as included in various vendors operating system distributions, could allow attackers to crash the vulnerable process or potentially execute arbitrary code.

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

[VulnWatch] iDefense Security Advisory 12.09.05: Ethereal OSPF Protocol Dissector Buffer Overflow Vulnerability

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.

III. ANALYSIS

Successful exploitation allows 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.

IV. DETECTION

iDefense has confirmed the existence of this vulnerability in the `ethereal-0.10.12` RPM from Red Hat Fedora Core 3. It is suspected that previous versions containing the OSPF dissector code are also vulnerable.

V. WORKAROUND

Disable the OSPF packet dissector in Ethereal by performing the following actions as the user invoking Ethereal, typically `root`.

Create the `.ethereal` directory:

```
# mkdir ~/.ethereal
```

You can safely ignore the following error:

[VulnWatch] iDefense Security Advisory 12.09.05: Ethereal OSPF Protocol Dissector Buffer Overflow Vulnerability

```
mkdir: cannot create directory '/root/.ethereal': File exists
```

Add the OSPF dissector to the list of protocols to ignore.

```
# echo ospf >> ~/.ethereal/disabled_protos
```

This workaround will prevent Ethereal from parsing the contents of OSPF packets, which prevents exposure to the vulnerability.

VI. VENDOR RESPONSE

A source patch is available from the main ethereal SVN Repository:

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

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2005-3651 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

VIII. DISCLOSURE TIMELINE

11/14/2005 Initial vendor notification
11/14/2005 Initial vendor response
12/09/2005 Public disclosure

IX. CREDIT

[VulnWatch] iDefense Security Advisory 12.09.05: Ethereal OSPF Protocol Dissector Buffer Overflow Vulnerability

The discoverer of this vulnerability wishes to remain anonymous.

Get paid for vulnerability research
<http://www.iDefense.com/poi/teams/vcp.jsp>

Free tools, research and upcoming events
<http://labs.iDefense.com>

X. LEGAL NOTICES

Copyright © 2005 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please email customerservice@xxxxxxxxxxxxx for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.