

[VulnWatch] iDefense Security Advisory 07.16.07: Trend Micro OfficeScan Session Cookie Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-07/msg00015.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxxx>
 - *Date:* Mon, 16 Jul 2007 18:57:05 -0400
-

Trend Micro OfficeScan Session Cookie Buffer Overflow Vulnerability

iDefense Security Advisory 07.16.07

<http://labs.iddefense.com/intelligence/vulnerabilities/>

Jul 16, 2007

I. BACKGROUND

Trend Micro OfficeScan is a centrally managed AntiVirus solution that allows administrators to manage virus and spyware protection in business environments. More information can be found on the vendors site at the following URL.

<http://us.trendmicro.com/us/products/enterprise/officescan-client-server-edition/>

II. DESCRIPTION

Remote exploitation of a stack-based buffer overflow vulnerability in Trend Micro Inc.'s OfficeScan for Windows could allow attackers to execute arbitrary code with the privileges of the IIS Web User.

The OfficeScan installation includes a series of CGI executables that are used for configuration through the Web interface. A shared library, CGICommon.dll, is used by many of these binaries to access environment variables passed to them from the parent IIS process. If a malicious Web request is made for a vulnerable binary, including an overly long session cookie, a stack-based Unicode buffer overflow will occur.

III. ANALYSIS

Exploitation allows attackers to execute arbitrary code with the permissions of the IIS Web user. Exploitation does not require authentication.

While the IIS Web user account is a limited account, this attack could be used to conduct further privilege escalation attacks.

IV. DETECTION

iDefense has confirmed this vulnerability in OfficeScan 7.3 with all current patches applied. Testing has shown that this attack can be conducted by requesting multiple CGI binaries that make use of the shared library. Other versions are suspected to be vulnerable.

V. WORKAROUND

iDefense is currently unaware of any workaround for this issue.

VI. VENDOR RESPONSE

Trend Micro has addressed this vulnerability by releasing the following patches for affected products.

CSM3.6 security patch 1149

CSM3.5 security patch 1152

CSM3.0 security patch 1209

<http://www.trendmicro.com/download/product.asp?productid=39>

OSCE 8.0 security patch 1042

OSCE 7.3 security patch 1293

OSCE 7.0 security patch 1364

OSCE 6.5 security patch 1364

OSCE 6.0 for SMB2.0 security patch 1398

<http://www.trendmicro.com/download/product.asp?productid=5>

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2007-3454 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

06/07/2007 Initial vendor notification

06/07/2007 Initial vendor response

07/16/2007 Coordinated public disclosure

IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

Get paid for vulnerability research

<http://labs.iddefense.com/methodology/vulnerability/vcp.php>

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

X. LEGAL NOTICES

Copyright © 2007 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 e-mail 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.