

[NT] Symantec Altiris Deployment Solution TFTP/MTFTP Service Directory Traversal Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-11/msg00001.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 1 Nov 2007 11:06:39 +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>

Symantec Altiris Deployment Solution TFTP/MTFTP Service Directory Traversal Vulnerability

SUMMARY

<<http://www.altiris.com/Products/DeploymentSolution.aspx>> Symantec Altiris Deployment Solution is "an automated OS deployment solution that is used for deploying and managing servers, desktops, and notebooks from a central location". Remote exploitation of a directory traversal vulnerability in Symantec's Altiris Deployment Solution products could allow attackers to gain read access to arbitrary files hosted on the Altiris server.

DETAILS

Vulnerable Systems:

- * Altiris Deployment Solution for Windows version 6.8 (pxemftftp.exe version 6.8.8297.48)

Immune Systems:

*

[NT] Symantec Altiris Deployment Solution TFTP/MTFTP Service Directory Traversal Vulnerability

Altiris Deployment Solution includes a tftp/mtftp server within its optional PXE server component which suffers from a directory traversal condition. The server runs with SYSTEM level privileges and allows unauthenticated attackers to download any file on the system.

Analysis:

Exploitation allows attackers to read arbitrary files from the server machine. The tftp/mtftp daemon runs with SYSTEM level privileges, so any file readable by SYSTEM with a known file path can be downloaded without authentication.

Workaround:

If the PXE server component is not required in your environment it should be disabled.

Vendor response:

Symantec Altiris has addressed this vulnerability by releasing a HotFix. More information is available in Symantec's advisory at the following URL:
<<http://www.symantec.com/avcenter/security/Content/2007.10.31.html>>
<http://www.symantec.com/avcenter/security/Content/2007.10.31.html>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3874>>
CVE-2007-3874

Disclosure timeline:

07/13/2007 – Initial vendor notification
07/16/2007 – Initial vendor response
10/31/2007 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense Labs.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=619>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=619>

=====

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.