

[NEWS] Netegrity SiteMinder Affiliate Agent Cookie Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0097.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/25/04

To: list@securiteam.com

Date: 25 Apr 2004 19:30:25 +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>

Netegrity SiteMinder Affiliate Agent Cookie Overflow

SUMMARY

The SiteMinder Affiliate Agent is a plugin that provides a connection from a main portal to an affiliate site without requiring a user to re-identify or provide additional information about them. The affiliate site can determine that the user has been registered at the main portal, and optionally, that the user has an active SiteMinder session.

The affiliate agent to determine if the user has been registered to the main portal uses the SMPROFILE cookie. Passing a large value to the SMPROFILE cookie can trigger a remotely exploitable heap overflow.

A Nessus (NASL) script, `siteminder_aa.nasl`, which can be used to scan for vulnerable servers, will be released after a 30 day delay.

Web servers that use the vulnerable SiteMinder plugin will quit responding to requests when the NASL script is executed.

DETAILS

Vulnerable Systems:

Securiteam: [NEWS] Netegrity SiteMinder Affiliate Agent Cookie Overflow

* SiteMinder Affiliate Agent 4.x

Vendor Response:

The handling of HTTP cookies has been modified to correctly process cookies of all sizes.

Please download and install the following package to apply the fix:
Web Agent 4QMR6 HF-016

The package is available at <<https://support.netegrity.com>>
<https://support.netegrity.com>

Please contact Netegrity Support for more information.

Toll-free Phone Number (U.S and Canada only): (877) 748-3646 (or 877-SITEMINDER)
International Phone Number: +1 (781) 663-7250 or +60 3 2055 3333

Notification Timeline:

- 4/07/2004 Vendor notified of issue
- 4/08/2004 Vendor confirms notification
- 4/14/2004 Vendor responds that they are fixing issue
- 4/21/2004 Vendor informs us that they have a patch available
- 4/22/2004 Advisory released

Recommendation:

Install the vendor supplied update.

Install an application level firewall that has cookie size filtering and restrict cookie sizes to less than 1024 bytes. This may effect other applications.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jjethro@si.rr.com>> Jeremy Jethro.

The original article can be found at:

<<http://www.atstake.com/research/advisories/2004/a042204-1.txt>>
<http://www.atstake.com/research/advisories/2004/a042204-1.txt>

=====

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@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

Securiteam: [NEWS] Netegrity SiteMinder Affiliate Agent Cookie Overflow

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.