

[NEWS] HP SIM 5.0 Session Fixation Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00030.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 21 May 2007 10:23:01 +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>

HP SIM 5.0 Session Fixation Vulnerability

SUMMARY

There is a session fixation vulnerability in HP Systems Insight Manager 4.2 and 5.0 SP4/5 (IM) that allows an attacker to gain administrative access to IM console. As a result, the attacker can take complete administrative control over all managed systems, upload and execute malicious code on them, extract any information from them and disable them at her will.

DETAILS

Vulnerable Systems:

- * HP Systems Insight Manager version 4.2
- * HP Systems Insight Manager version 5.0 SP4
- * HP Systems Insight Manager version 5.0 SP5

Immune Systems:

- * HP Systems Insight Manager version 5.1

The Systems Insight Manager web application is using a JSESSIONID session cookie for maintaining a session with administrator's browser. Apparently, the console is vulnerable to session fixation and allows an attacker to

[NEWS] HP SIM 5.0 Session Fixation Vulnerability

obtain the session cookie, fix it on administrator's browser and thus force him to use that cookie when subsequently logging into the administration console. Once the administrator is logged in, the attacker can use the same cookie to enter the already logged-in session and assume the identity of the administrator.

After gaining administrative rights, an attacker can do anything the administrator could do, including executing arbitrary commands on all managed computers. In SIM Service Pack 4, a new cookie JSESSIONIDSSO was introduced to fix this issue; however, it was possible to bypass checks for the JSESSIONIDSSO cookie and thus still attack the SIM administrator with a fixed JSESSIONID cookie.

Solution:

HP has released a newer version of SIM (SIM 5.1) which fixes this issue.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:lists@xxxxxxxx>> ACROS Security.

The original article can be found at:

<<http://www.acrossecurity.com/aspr/ASPR-2007-05-14-1-PUB.txt>>

<http://www.acrossecurity.com/aspr/ASPR-2007-05-14-1-PUB.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@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.