

[UNIX] Mod_Survey ENV Tag Security Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0086.html>

From: support@securiteam.com

Date: 03/29/03

From: support@securiteam.com

To: list@securiteam.com

Date: 29 Mar 2003 20:00:48 +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

In the US?

Contact Beyond Security at our new California office
housewarming rates on automated network vulnerability
scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Mod_Survey ENV Tag Security Vulnerability

SUMMARY

<<http://gathering.itm.mh.se/modsurvey/>> Mod_Survey is an Apache module that displays and handles questionnaires written in a special XML-based markup language. Mod_Survey is primarily targeted towards Linux/Unix, but is possible to run in Windows.

If ENV tags are used in surveys it is, under certain circumstances, possible for an outside evil person to send arbitrary data to the data handling system. This could corrupt the data repository or, in the case of badly configured RDBMSs, be used to execute arbitrary database commands.

This only affects survey files where ENV tags are used.

DETAILS

Vulnerable systems:

All versions from version 3.0.9 up to (but not including) 3.0.14e and 3.0.15-pre6 are vulnerable. Thus, the following versions have the problem:

* 3.0.9

- * 3.0.10
- * 3.0.11
- * 3.0.12
- * 3.0.13
- * 3.0.14
- * 3.0.14d
- * 3.0.15-pre1
- * 3.0.15-pre2
- * 3.0.15-pre3
- * 3.0.15-pre4
- * 3.0.15-pre5

Immune systems:

Versions 3.0.8 and earlier

- * 3.0.14e
- * 3.0.15-pre6

In version 3.0.9, ENV tags were introduced as a way to submit data from the environment to the data repository along with the actual questionnaire answers. This is, when used at all, usually used for gathering info such as from which IP the respondent has connected, or which user agent the respondent is using.

So far, this data has been sent unchecked to the data sub system. However, a malicious user could easily construct some of the most common environment variables and thus send arbitrary data to the system.

One example would be if the survey author is using an ENV tag with the field HTTP_USER_AGENT. The evil cracker could then change this string in his browser to something that he knew would corrupt the data repository, such as the delimiting character for ASCIIFILE/AUTODATA save methods or meta characters for the DBI save method.

In versions 3.0.14e and 3.0.15-pre6, this has been solved through the encoding of the environment string. With this, encoding all "dangerous" characters are encoded to %XX where XX is the character's hex code. Thus, a semi-colon is submitted as %1B rather than as a semi-colon.

Exploit:

Anyone can exploit this by changing the user_agent string in his browser.

Impact:

There are several points limiting the impact of the problem: The ENV tag must be actively chosen and inserted by a survey author for the above to be a problem. Secondly, most fields are not possible to change from the outside as they are set by Apache. Thirdly, unless access is given to the source of the survey, there is no way to know from the outside whether an ENV tag is used at all.

Solution:

For systems with 3.0.14d or earlier installed, upgrade to 3.0.14e. For

Securiteam: [UNIX] Mod_Survey ENV Tag Security Vulnerability

systems with versions from 3.0.15-pre1 to -pre5, upgrade to 3.0.15-pre6.

If you only have trusted users on the system, you can also simply refrain from using ENV tags. Surveys that do not include the ENV tags are not vulnerable.

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://gathering.itm.mh.se/modsurvey/SA20030323.txt>>

<http://gathering.itm.mh.se/modsurvey/SA20030323.txt>

The information has been provided by <<mailto:joel.palmius@mh.se>> Joel Palmius and Nicklas Deutschmann.

=====

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

=====

=====

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.