

[NEWS] Mod_Survey SYSBASE Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0008.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/05/03

To: list@securiteam.com

Date: 5 May 2003 18:39:29 +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 SYSBASE 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 also possible to run in Windows. In all versions prior to 3.0.15-stable, it is possible for a remote attacker to fill the partition on which the central data repository resides, through sending access requests to non-existing surveys.

DETAILS

Vulnerable systems:

- * Mod_Survey versions prior to 3.0.15-stable

Immune systems:

- * Mod_Survey version 3.0.15-stable

Solution:

All users are encouraged to upgrade to version 3.0.15-stable. However, if you are running 3.0.14 - 3.0.14e and do not wish to upgrade at this time,

Securiteam: [NEWS] Mod_Survey SYSBASE Vulnerability

you could also download the "Document.pm" module from the mod_survey homepage (<<http://gathering.itm.mh.se/modsurvey/>> <http://gathering.itm.mh.se/modsurvey/>) and use it to replace the faulty one in the "Survey" subdir of the installation folder. This is not an option if you run versions prior to 3.0.14.

Apache needs to be stopped (to a full stop, not "graceful") and then started again before changes in these modules take effect.

Technical details:

Mod_survey does per default store all data files, such as cache, keys and submitted questionnaire answers, in a data repository, "SYSBASE". In practice, this repository is a subdir of the central data repository.

SYSBASE is created when the survey file is first accessed, and is given the full path of the survey as name (with slashes converted to underscores).

Unfortunately, the check whether the survey file actually exists did not take place until *after* the repository was initialized. Thus, an empty SYSBASE would be set up even if the access concerned a non-existent survey file.

In normal operation, this might look rather sloppy, but would not be a problem, since the occasional mistyped path would only result in an additional empty directory. However, while the directory is "empty" in the sense that it does not contain any data from the beginning, it still occupies space in the file system. A script with a loop that produces access requests to new non-existent surveys several times per second would soon fill the partition.

The consequences of this differ depending on which platform the system is installed, and which partition contains the data repository. The usual consequence would simply be that no data could be written to the partition, thus stopping further data collection. However, in theory, a filled partition could down a system. An example would be on a unixoid system where the data repository resided somewhere in /var (the default location is in /usr/local/mod_survey/data).

Impact:

All current installations of mod_survey are vulnerable and could thus at least be attacked with a DoS attack exploiting the above.

It is conceivable that the problem could also be used to attack bugs in the file system itself, as an example through injecting control chars that the operating system cannot handle, although no exploit for this has yet been proposed. An upgrade to 3.0.15-stable removes the theoretical possibility for this problem too though.

ADDITIONAL INFORMATION

Securiteam: [NEWS] Mod_Survey SYSBASE Vulnerability

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

=====

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.