

[UNIX] Greymatter Remote Login / Password Exposure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0139.html>

From: support@securiteam.com

Date: 02/25/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 25 Feb 2002 14:27:28 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Greymatter Remote Login / Password Exposure

SUMMARY

<<http://noahgrey.com/greysoft/>> Greymatter is the original -- and still the world's most popular -- open source web logging and journal software. A security vulnerability in the product allows remote attackers to retrieve the main author name, and password. This enables the attacker to gain full control over the program.

DETAILS

Where the vulnerability lies:

Just search for a file called "gmrightclick" and download a file called "gmrightclick*.reg" where the stars represent a number. Open it and there you have it: Username and Password.

When does it happen?

If the administrator uses the "Add Bookmarklets" feature to add a link/photo, it will add a new "gmrightclick*" file unless they have set the "clear" function in their configuration. After adding a link, they need to hit the "Clear And Exit" button at the bottom of the page. This will remove all "gmrightclick*.reg" files.

Securiteam: [UNIX] Greymatter Remote Login / Password Exposure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jericho@attrition.org>>
security curmudgeon.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] L1lHTTP Web Server Protected File Access Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)