

[UNIX] RNN's Guestbook Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0007.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/03/03

To: list@securiteam.com

Date: 3 Dec 2003 15:07:05 +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>

RNN's Guestbook Multiple Vulnerabilities

SUMMARY

<<http://www.cbvfd.com/rnn/scripts/guestbook.htm>> RNN Guestbook is "an easily customizable CGI script that allows visitors to post messages for others to read". Multiple vulnerabilities have been found in the product, they allow remote command execution, administrative access gaining, information disclosure (reading of files), arbitrary HTML insertion/script injection and plain text administrative password disclosure.

DETAILS

Vulnerable systems:

- * RNN Guestbook version 1.2

Administrative Access Vulnerabilities

If an attacker was to visit `~/gbadmin.cgi`, he/she would be prompted for a password. But if that same attacker was to go directly to the `QUERY_STRING` and fill in the values for "action", he/she could have total control over the guestbook without the need of any authentication.

Examples:

1. `~/gbadmin.cgi?action=change_adminpass` – Change password
2. `~/gbadmin.cgi?action=delete_guests` – Delete ALL posts on the guestbook.

Securiteam: [UNIX] RNN's Guestbook Multiple Vulnerabilities

3. ~/gadmin.cgi?action=setup – Change setup information for guestbook.
4. ~/gadmin.cgi?action=colors – Modify the look and feel of the guestbook
5. ~/gadmin.cgi?action=change_automail – Change emailing information

Information Disclosure Vulnerability (Reading of Files)

By taking advantage of the Administrative Access Vulnerabilities, an attacker could visit ~/gadmin.cgi?action=setup and change the "guestbook entry file" path to point towards any file (EX: /etc/passwd) on the system readable by the account in which the HTTPd is running. After making this change, the attacker would view guestbook.cgi not to read POSTs, but to read the contents of the file above.

Remote Command Execution

Also by taking advantage of the Administrative Access Vulnerability, instead of an attacker changing the guestbook entry file path to something such as /etc/passwd to read that file's contents, an attacker can insert /path/file;<cmd> <args>| resulting in the execution of the cmd at the end of /path/file.

Example:

```
/etc/passwd;touch /tmp/hacked|
```

Arbitrary HTML Insertion / Script Injection Vulnerabilities

Due to improper filtering, all the scalars below allow the insertion of HTML tags, making guestbook.cgi vulnerable to script injection.

Even though the gadmin.cgi offers the option to not allow HTML tags in the \$comment field, HTML tags are still accepted.

```
sub process_input {
# process variables
$name = "$in{'name'}";
$email = "$in{'email'}";
$refer = "$in{'refer'}";
$msn = "$in{'msn'}";
$aol = "$in{'aol'}";
$guest_site = "$in{'guest_site'}";
$comment = "$in{'comment'}";
$ip = "$in{'ip'}";
&validate_input;
```

Plain Text Administrative Password

The administrative password can be found in the gpass.pl file also found in the same directory as the rest of the guestbook. Combine the permissions recommended by the author in "readme.txt" and the plain text password, any "local" users can view the plain text password found in gpass.pl.

Vendor status:

10-11-03 – Sent an email to webmaster at cbvfd.com "ATT: Mike Reed (author)" (No Reply)

Securiteam: [UNIX] RNN's Guestbook Multiple Vulnerabilities

- 10-12-03 – Sent an email to Mike Reed at mike at cbvfd.com (No Reply)
- 10-16-03 – Sent another email to mike at cbvfd.com (No Reply)
- 10-19-03 – Sent email to (Mike's other email) zmlr15 at imail.etsu.edu.
(Failed Recipient)
- 10-20-03 – Posted a msg on the cbvfd.com msgboard. (No Response Yet)
- 10-20-03 – Called Mike via phone. (No Answer)
- 10-25-03 – Sent an email to another one of Mike's addresses. reed2323 at cbvfd.com
- 10-26-03 – Received an email from Mike and replied with a a copy of this advisory.
- 11-26-03 – No word from author since he had received a copy of this advisory. Releasing information.

ADDITIONAL INFORMATION

The information has been provided by <mailto:brainrawt@haxworx.com> Chris Rahm (aka: BrainRawt).

=====

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.