

[UNIX] Bogofilter Contrib/Bogopass Temp File Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0005.html>

From: support@securiteam.com

Date: 12/01/02

From: support@securiteam.com

To: list@securiteam.com

Date: 1 Dec 2002 15:06:49 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Bogofilter Contrib/Bogopass Temp File Vulnerability

SUMMARY

<<http://bogofilter.sourceforge.net/>> Bogofilter is a software package to determine if a mail on its standard input is SPAM or not. A vulnerability in the product allows local attackers to gain elevated privileges.

DETAILS

Vulnerable systems:

- * Bogofilter version 0.9.0.4

Immune systems:

- * Bogofilter version 0.9.0.3 and prior
- * Bogofilter version 0.9.0.5 and newer

A vulnerability was found in the contrib/bogopass Perl program that was added to bogofilter as of the 0.9.0.4 beta release (date: 2002-11-27 23:04:28 UTC in CVS) with bogofilter, but is not installed by default.

The bogopass program creates temporary files with the name /tmp/bogopass.\$\$, where \$\$ is the process ID, with the open FH, ">file" syntax of Perl, which uses O_TRUNC mode, not O_EXCL.

Securiteam: [UNIX] Bogofilter Contrib/Bogopass Temp File Vulnerability

Impact:

This vulnerability allows for anonymous file destruction or change, and might be abused to further escalate the privileges of the local attacker.

If bogopass is run by the root user, this may eventually lead to a complete system compromise.

Workaround:

Do not install or use the "bogopass" program that shipped with the vulnerable versions (see above) of bogofilter.

Solution:

Upgrade your bogofilter to version 0.9.0.5 beta, and reinstall the bogopass program. Make sure you delete all copies of the old version of bogopass.

bogofilter 0.9.0.5 is available from SourceForge:

http://sourceforge.net/project/showfiles.php?group_id=62265&release_id=118794tp://sourceforge.net/project/showfi

Solution details:

* revision 1.3

date: 2002/11/28 03:32:47; author: m-a; state: Exp; lines: +67 -26

Other hints:

Software that treats user input should not run as root if it can be avoided. When installing bogofilter for system-wide use, make sure that it runs as an unprivileged user to limit the impact of possible vulnerabilities.

ADDITIONAL INFORMATION

The information has been provided by <mailto:matthias.andree@gmx.de>
Matthias Andree.

=====

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.