

[UNIX] DSPAM Default Permissions Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0048.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/16/03

To: list@securiteam.com

Date: 16 Sep 2003 16:00:12 +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>

DSPAM Default Permissions Vulnerability

SUMMARY

<<http://www.nuclearelephant.com/projects/dspam/>> DSPAM is "an advanced anti-spam solution compatible with most UNIX email server implementations. DSPAM combines deobfuscation techniques, token chains, and Bayesian statistical analysis to create a very effective anti-spam engine capable of teaching itself. DSPAM masquerades as the system's local delivery agent and performs analysis on a per-user basis".

Due to the default permissions set by the product, it is possible for a local attacker to gain elevated privileges by executing the DSPAM program from the command line (the privileges given to the DSPAM product).

DETAILS

Vulnerable systems:

- * DSPAM version 2.6.5
- * DSPAM version 2.6.5.1

Immune systems:

- * DSPAM version 2.6.5.2
- * DSPAM version 2.7.0.beta.3

Securiteam: [UNIX] DSPAM Default Permissions Vulnerability

In order for the DSPAM agent to function correctly, when called by the quarantine CGI or by some MTAs that drop privileges prior to calling dspam, the dspam agent must be setgid to have access to its own data. In most installations, DSPAM runs under the group 'mail'.

DSPAM v2.6.5 introduced a new feature providing the ability to change the delivery agent and quarantine agents via command line. Due to the default installation permissions of DSPAM, however, this functionality was provided to any users capable of executing the DSPAM agent enabling them to run commands in this new group.

Solution:

Unset the world-execute bit of the DSPAM agent's file permissions, or upgrade to v2.6.5.2. Alternatively, users that are more daring may try v2.7.0.beta.3, which incorporates trusted user security.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:jonathan@nuclearelephant.com> Jonathan A. Zdziarski.

=====

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.