

[NT] Winmail Server Information Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0080.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/22/04

To: list@securiteam.com

Date: 22 Dec 2004 14:09:48 +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>

Winmail Server Information Disclosure

SUMMARY

<<http://www.magicwinmail.net>> Winmail Server is "an enterprise class mail server software system offering a robust feature set, including extensive security measures. Winmail Server supports SMTP, POP3, IMAP, Webmail, LDAP, multiple domains, SMTP authentication, spam protection, anti-virus protection, SSL/TLS security, Network Storage, remote access, Web-based administration, and a wide array of standard email options such as filtering, signatures, real-time monitoring, archiving, and public email folders".

Several scripts (chgpwd.php, domain.php and user.php) that come with Winmail Server have been found to disclose sensitive information on the remote hosts.

DETAILS

Vulnerable Systems:

* Winmail Server version 4.0 (Build 1112)

Exploit:

Access the following URL: <http://127.0.0.1:6080/admin/chgpwd.php>, as an alternative you can try and access the following pages domain.php,

Securiteam: [NT] Winmail Server Information Disclosure

user.php found under the same directory.

Workaround:

You can edit c:\windows\winmail_php.ini change:

display_errors = On

To

display_errors = Off

ADDITIONAL INFORMATION

The information has been provided by <mailto:gss_it@yahoo.com> GSS IT.

=====

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.