

[NT] Deeply nested OWA Request Can Consume Server CPU Availability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-09/0087.html>

From: support@securiteam.com

Date: 09/27/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] Deeply nested OWA Request Can Consume Server CPU Availability

Message-Id: <20010927122315.167EF138BF@mail.der-keiler.de>

Date: Thu, 27 Sep 2001 14:23:15 +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.

Deeply nested OWA Request Can Consume Server CPU Availability

SUMMARY

Exchange 2000 Outlook Web Access accepts and processes requests for items in an authenticated user's mailbox without verifying first that the folder structure is valid. This enables a remote attacker to mount a denial of service attack by repeatedly levying a request for a non-existent but deeply nested folder in his own mailbox.

Exploiting the vulnerability would not necessarily affect the OWA server itself. The effect of the vulnerability would be to cause the process servicing the attacker's mailbox to consume most or all of the CPU availability on the server it was running on. In many cases, this process would run on the OWA server, and thus the effects would be seen there. However, if the process servicing the attacker's mailbox ran on a back-end server, the effect of exploiting the vulnerability would be seen there. In any event, the affected server would resume normal service once the request was handled.

DETAILS

Securiteam: [NT] Deeply nested OWA Request Can Consume Server C

Vulnerable systems:

- * Microsoft Exchange 2000 Server Outlook Web Access

Mitigating factors:

- * Only users who could authenticate to the server could exploit this vulnerability.
- * The attacker would need to have permissions on at least one mailbox in order to exploit the vulnerability.
- * The user can only perform this task against mailboxes to which they have permission.
- * The vulnerability could not be used to cause the mailbox store to fail, or to corrupt mailbox data.

Patch availability:

Download locations for this patch

- * Microsoft Exchange 2000:

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32431>
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32431>

What is the scope of the vulnerability?

This is a denial of service vulnerability. An attacker who exploited this vulnerability could temporarily consume most or all of the resources on mail server, slowing or preventing other users from accessing their mail.

The vulnerability would not allow the attacker to add, delete, change, or view anyone else's mail. In order to exploit the vulnerability, the attacker would need to be authorized to access at least one mailbox on the server. The effects of exploiting the vulnerability would be temporary, and the server would resume normal operation once the attack ceased.

What causes the vulnerability?

The vulnerability results because Exchange 2000 OWA does not limit how complex an authenticated user's request to the server can be. By constructing an extremely complex request, a user could consume all CPU availability on the server that processes the request item.

What is OWA?

OWA is a feature in Exchange 5.5 and 2000 that allows users to access their email via a web browser instead of a mail client. Essentially, OWA makes an Exchange server also function as a web site that lets authorized users read or send mail, manage their calendar, or perform other mail functions via the Internet.

What is wrong with OWA?

When OWA processes a request from a user to access a particular mail folder, it does not verify first that the folder actually exists. By levying a request involving an extremely complex folder structure – for instance, a folder nested ten thousand folders deep in a tree – it would be possible to make the server spend an inordinate amount of time processing that request.

Securiteam: [NT] Deeply nested OWA Request Can Consume Server C

Would the folder have to actually exist?

No, the requested item does not have to be valid. Any very deeply nested request can exploit this vulnerability.

What would this vulnerability allow the attacker to do?

By repeatedly sending requests that involve deeply nested folders, the attacker could monopolize the server's CPU availability, thereby slowing the server's response or making it completely unresponsive until the request had been completed.

How long would the effects of exploiting the vulnerability last?

It would depend on how complex the request was. However, whenever it completed processing the request, service would return to normal.

How many servers could this affect?

It would depend on how the specific server was configured. OWA sends requests to the process that controls the user's mailbox. If the process were located on the same server as OWA, only the OWA server would be affected. On the other hand, if the process were located on another server, that server, rather than the OWA server, would be affected. This patch should only be applied to Exchange servers that host user mailboxes.

Who could exploit this vulnerability?

Only user who was able to authenticate to the mail server could exploit this vulnerability, and even then only if he had been given access to a mailbox on it.

Could the vulnerability be used to gain any control over the server?

No. The rogue user could only exploit this as a denial of service. The rogue user must be an authenticated user.

I have an Exchange Server, but I do not offer OWA? Do I need the patch?

No. Only Exchange servers with OWA need to be patched.

What does the patch do?

The patch eliminates the vulnerability by restricting the maximum depth of a nested request by an authenticated user.

ADDITIONAL INFORMATION

The information has been provided by <mailto:secnotif@MICROSOFT.COM>
Microsoft Product Security.

=====

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

Securiteam: [NT] Deeply nested OWA Request Can Consume Server C

=====
=====

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: "[\[UNIX\] Security Vulnerability in PHP-Nuke Allows File Copying \(admin.php\)](#)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)