

[NT] Vulnerability in Exchange Server 5.5 Outlook Web Access Allows CSS and Spoofing Attacks (MS04-026)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0032.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/11/04

To: list@securiteam.com

Date: 11 Aug 2004 15:15:43 +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>

Vulnerability in Exchange Server 5.5 Outlook Web Access Allows CSS and Spoofing Attacks (MS04-026)

SUMMARY

This update resolves a newly discovered, privately reported vulnerability. A cross-site scripting and spoofing vulnerability exists in Outlook Web Access for Exchange Server 5.5 that could allow an attacker to convince a user to run a malicious script.

An attacker who successfully exploited the vulnerability could manipulate Web browser caches and intermediate proxy server caches, and put spoofed content in those caches. They may also be able to exploit the vulnerability to perform cross-site scripting attacks.

DETAILS

Affected Software:

* Microsoft Exchange Server 5.5 SP4

Non-Affected Software:

* Microsoft Exchange 2000 Server

Securiteam: [NT] Vulnerability in Exchange Server 5.5 Outlook Web Access Allows CSS and Spoofing Attacks (MS04-008)

* Microsoft Exchange Server 2003

Affected Components:

* Outlook Web Access –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=66E4E033-5A4C-4EEC-84F1-31F0CA878092&display=details>
Download the update

This is a cross-site scripting and spoofing vulnerability. The cross-site scripting vulnerability could allow an attacker to convince a user to run a malicious script. If this malicious script is run, it would execute in the security context of the user. Attempts to exploit this vulnerability require user interaction. This vulnerability could allow an attacker access to any data on the Outlook Web Access server that was accessible to the individual user.

It may also be possible to exploit the vulnerability to manipulate Web browser caches and intermediate proxy server caches, and put spoofed content in those caches.

Workaround:

Microsoft has tested the following workarounds: