

[NT] Microsoft Windows 2003 Outlook Web Access URL Injection Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0085.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/17/05

To: list@securiteam.com

Date: 17 Mar 2005 18:55:29 +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>

Microsoft Windows 2003 Outlook Web Access URL Injection Vulnerability

SUMMARY

By using specially crafted URL an attacker can cause a user using Microsoft's Windows 2003 Outlook Web Access (OWA) to redirect to an arbitrary URL.

DETAILS

Vulnerable Systems:

* Microsoft Windows 2003 Outlook Web Access (OWA)

A vulnerability in Microsoft Windows 2003 Outlook Web Access allows malicious attackers to redirect the login to any URL they wish. This allows the attacker to force the user to the site of the attackers choosing enabling the attacker to use social engineering and phishing style of attacks.

An attacker could also use this attack to gather valid user email addresses, by appending an obfuscated redirected URL with a encoded URL such as

[https://\[owa-host\]/exchweb/bin/auth/owalogon.asp?url=http://3221234342/](https://[owa-host]/exchweb/bin/auth/owalogon.asp?url=http://3221234342/)

Securiteam: [NT] Microsoft Windows 2003 Outlook Web Access URL Injection Vulnerability

Proof of Concept:

1. [https://\[owa-host\]/exchweb/bin/auth/owalogon.asp?url=http://\[otherhost\]](https://[owa-host]/exchweb/bin/auth/owalogon.asp?url=http://[otherhost])
2. Click "login"
3. After the injection into the form, the source reveals:
< BODY scroll="AUTO" bgColor="#3D5FA3" text="#000000" leftMargin=0
topMargin=0>
< FORM action="/exchweb/bin/auth/owaauth.dll" method="POST"
name="logonForm" autocomplete="off">
< INPUT type="hidden" name="destination" value="http://[otherhost]">
< INPUT type="hidden" name="flags" value="0">
< TABLE id="borderTable" class="standardTable" cellSpacing=0 cellPadding=0
height="100%" width="100%" bgColor="#3D5FA3" border=0>

ADDITIONAL INFORMATION

The information has been provided by <mailto:se_cur_ity@hotmail.com>
morning_wood.

=====

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.