FORTCONSULT

Straight talk on IT security

SECURITY ADVISORY

ID: FCSA1205

Microsoft Outlook WebApp

Open Redirection (OWASP - Unvalidated Redirects and Forwards)

Phone: +45 70207525 Email: info@fortconsult.net Web: www.fortconsult.net

Background

From the Microsoft website:

"Exchange 2010 and Microsoft Outlook Web App deliver a rich, familiar web-based email experience that allows you to:

Access email, voicemail, instant messages, and SMS text messages directly from your inbox using any of the major web browsers (Internet Explorer, Safari, Firefox, and Chrome)

Use Conversation View to see messages in context, making it easier to manage email more efficiently and reduce inbox overload

Share your calendar with colleagues both inside and outside the organization

Check other users' availability with the presence indicator and choose the best mode of communication—email, instant message, or SMS"

From wikipedia:

"Outlook Web App (OWA), originally called Outlook Web Access and before that Exchange Web Connect (EWC), is a webmail service of Microsoft Exchange Server 5.0 and later. Outlook Web App comes as a part of Microsoft Exchange Server or Microsoft Office 365."

Description

An open redirect is an application that takes a parameter and redirects a user to the parameter value without any validation. This vulnerability is used in phishing attacks to get users to visit malicious sites without realizing it. (OWASP).

Analysis

Attacker links to unvalidated redirect and tricks victims into clicking it. Victims are more likely to click on it, since the link is to a valid site. Attacker targets unsafe forward to bypass security checks.

Attackers are usually redirects users to malicious websites.

Avoiding such flaws is extremely important as they are a favorite target of phishers trying to gain the user's trust.

Exploit

(tested on)

Version: 14.1.287.0

Client Access server version: 14.1.218.0

Mailbox server Microsoft Exchange version: 14.1.218.0

Should be valid for the latest and patched version at June 2012.

Original link:

https://exchange.funnytest.com/owa/redir.aspx?C=5gsljn5jyfnak5ecjngakj5ngakj5gk4&URL=https%3a%2f%2fwww.notfunnytest.org%2fdocs%2finformation.pdf

Malicious link:

https://exchange.funnytest.com/owa/redir.aspx?C=5gsljn5jyfnak5ecjngakj5ngakj5gk4&URL=https%3a%2f%2fwww.MALICIOUS.org%2fdocs%2finformation.pdf

CVE Reference

N/A at the release time.

Recommendations

1. Preform input validation.

Disclosure Timeline

14 June 2012 – Vulnerability found.

14 June 2012 – Vendor Notification.

15 June 2012 – Vendor ACK back, opened a case.

29 June 2012 – ACKed the vendor for a fix date.

29 June 2012 – Vendor reply “The above strikes me as not being an open redirect at all. Can you elaborate on a scenario where this could actually be used as an open redirect?”.

2 July 2012 – Public Disclosure, we will let the public decide if it can be used.

The Security Research Team

This advisory has been discovered by FortConsult’s Security Research Team/Yaniv Miron.

About FortConsult

FortConsult provides independent security assessment services, including penetration testing and PCI DSS assessment service internationally to customers, such as financial services companies, banks, acquirers, service providers and merchants.

See www.fortconsult.com for more information about FortConsult.

Or contact us at +45 7020 7525 or info@fortconsult.net.

Copyright and Disclaimer