Advisory	**EXX-2021-01**		January 21, 2021
Manufacturer	Vodafone	Product	Unitymedia email verification
Affected Version(s)	N/A	Tested Version(s)	N/A
CWE	CWE-601: URL redirection to untrusted site	CVE	N/A
Risk	MEDIUM	Status	ACTIVE

Overview

[1] The URL http://scb.unitymedia.de/click?redirect_to= is vulnerable to the Open Redirect vulnerability (CWE-601) This URL is used by Vodafone to redirect customers to a verification page, but using any host name as parameter, it can be abused for phishing, redirecting users to malicious websites.

Vulnerability Details

URL redirection to untrusted site allows an attacker, to redirect a victim to a page the victim does not want to visit, resulting in phishing. An attacker prepares an email containing this Unitymedia URL to make it appear as a legit Vodafone/Unitymedia email. The attacker redirects the victim to a phishing page and tries to obtain credentials.

Proof of Concept (PoC)

Call http://scb.unitymedia.de/click?redirect_to= with any host name, for example http://scb.unitymedia.de/click?redirect_to=www.exxeta.com

Solution

The redirect_to parameter needs to be checked on the server side. A temporary solution for clients is to check the redirect_to parameter for conspicious values.

Disclosure Timeline

2020-12-21	Discovery of the open redirect
2020-12-21	Open redirect reported to Vodafone
2021-01-22	Advisory published

References

[1] REF Description
https://exxeta.com

Credits

This security vulnerability was found by Sebastian Schwegler of EXXETA.
E-Mail: sebastian.schwegler@exxeta.com

Disclaimer

The information provided in this security advisory is provided ”as is” and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible. The latest version of this security advisory is available on the EXXETA website.

Copyright