	Authorisation. Jason Edelstein
	Release date. 30 October 2014

Sense of Security – Security Advisory – SOS-14-003.

Cisco CUCDM Self Care Portal Multiple Vulnerabilities

30 October 2014.

Sense of Security	Authorisation. Jason Edelstein
	Release date. 30 October 2014

Cisco CUCDM Self Care Portal - Security Advisory - SOS-14-003

Release Date.	30-Oct-2014
Last Update.	-
Vendor Notification Date.	17-Jan-2014
Product.	Cisco Unified Communications Domain Manager
Platform.	-
Affected versions.	-
Severity Rating.	Medium
Impact.	Hijacking Cross-site Scripting
Attack Vector.	Remote with / without authentication
Solution Status.	Vendor patch
CVE reference.	CVE-2014-3283
Cisco references.	https://tools.cisco.com/bugsearch/bug/CSCum75078/ http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3283

Details.

Multiple medium risk security vulnerabilities were detected in the Self Care portal of the Cisco Unified Communications Domain Manager (a.k.a. CUCDM or VOSS Solutions Domain Manager). The security vulnerabilities can be used to obtain unauthorised access to the CUCDM Self Care portal and to compromise the hosted VoIP tenant services. Fatih Ozavci, a Senior Security Consultant with Sense of Security, has demonstrated these vulnerabilities and additional design issues at Black Hat USA 2014 and Def Con 22 security events using the Viproy VoIP Penetration Testing Kit.

Details of the vulnerabilities and required security fixes or workarounds can be found within the following references:

1. Cisco Unified Communications Domain Manager Stored XSS Vulnerability (Medium Risk)

https://tools.cisco.com/bugsearch/bug/CSCum75078/

CUCDM is not properly validating some HTML parameter input. An attacker could exploit this issue to store a malicious payload that could then be executed by other users of the system

Conditions:

The attacker needs to have valid credentials in order to perform the attack, and needs to convince valid user to execute some actions.

2. Cisco Unified Communications Domain Manager Self-Care HTTP Redirect Vulnerability (Low Risk)

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3283

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3283

A vulnerability in the web framework of the VOSS Operating System running on the Cisco Unified Communications Domain Manager (Cisco Unified CDM) Application Software could allow an unauthenticated, remote attacker to inject a crafted HTTP header that could cause a web page to redirect to a possible malicious website.

The vulnerability is due to insufficient validation of user input before using it as an HTTP header value on VOSS Self-Care Client Portal applications. An attacker could exploit this vulnerability by convincing a user to access a crafted URL.

Exploits and Tools.

Viproy VoIP Penetration Testing and Exploitation Kit:

http://www.viproy.com

Solution.

All vendor security fixes must be installed.

Discovered by.

Fatih Ozavci from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and

architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-14-003.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php