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

Sense of Security – Security Advisory – SOS-14-002.

Cisco CUCDM Administration Portal Multiple Vulnerabilities

30 October 2014.

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

Cisco CUCDM Administration Portal - Security Advisory - SOS-14-002

Release Date.	30-Oct-2014
Last Update.	-
Vendor Notification Date.	17-Jan-2014
Product.	Cisco Unified Communications Domain Manager
Platform.	-
Affected versions.	-
Severity Rating.	High / Medium / Low
Impact.	Privilege escalation Security bypass Exposure of sensitive information
Attack Vector.	Remote with / without authentication
Solution Status.	Vendor patch Vendor workaround
CVE reference.	CVE-2014-2197 CVE-2014-3277 CVE-2014-3279 CVE-2014-3280 CVE-2014-3282
Cisco references.	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140702-cucdm http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3277 http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3279 http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3280

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3282

Details.

Multiple high risk security vulnerabilities were detected in the administration 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 services, to bypass the authorisation scheme, to elevate the current user privileges and to compromise the hosted VoIP services and infrastructure. 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 Privilege Escalation Vulnerability (High Risk)

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140702-cucdm

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2197

A vulnerability in the web framework of the Cisco Unified Communications Domain Manager Application Software could allow an authenticated, remote attacker to elevate privileges and gain administrative access to the affected system.

The vulnerability is due to improper implementation of authentication and authorisation controls within the Administration GUI. An attacker could exploit this vulnerability by submitting a crafted URL to change the administrative credentials of a user. The attacker needs to be authenticated to the system or convince a valid user of the Administration GUI to click a malicious link.

2. Cisco Unified Communications Domain Manager Admin Information Disclosure Vulnerability (Low Risk)

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3277

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3277

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 authenticated, remote attacker to access information about users and user groups.

The vulnerability is due to improper implementation of authentication and authorisation controls of the VOSS Administration GUI. An attacker could exploit this vulnerability by submitting a crafted URL to execute administrative tasks. The

attacker must be authenticated as a Location Administrator or must convince a user with Location Administrator privileges to click a malicious link.

3. Cisco Unified Communications Domain Manager Admin User Enumeration Vulnerability (Medium Risk)

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3279

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3279

A vulnerability in the web framework of the VOSS Operating System running on Cisco Unified Communications Domain Manager (Cisco Unified CDM) Application Software could allow an unauthenticated, remote attacker to enumerate valid user accounts.

The vulnerability is due to improper implementation of authentication and authorisation controls when accessing certain web pages of the Administration GUI. An attacker could exploit this vulnerability by submitting a crafted URL to the affected system.

4. Cisco Unified Communications Domain Manager Admin Information Disclosure Vulnerability (Low Risk)

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3280

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3280

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 authenticated, remote attacker to access certain user information.

The vulnerability is due to improper implementation of authentication and authorisation controls when accessing certain web pages of the Administration GUI. An attacker could exploit this vulnerability by submitting a crafted URL to the affected system.

5. Cisco Unified Communications Domain Manager Admin Number Translation Information Disclosure Vulnerability (Low Risk)

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3282

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3282

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 authenticated, remote attacker to access information about number translation.

The vulnerability is due to improper implementation of authorisation controls when accessing certain web pages of Administration GUI applications. An attacker could exploit this vulnerability by submitting a crafted URL to the affected system. The

attacker would need the privileges of a Location Administrator user to exploit this vulnerability.

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-14-002.pdf

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

Other Sense of Security advisories can be found at:

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