Sense of Security – Security Advisory – SOS-14-001.

Cisco CUCDM IP Phone Services Multiple Vulnerabilities

30 October 2014.

Cisco CUCDM IP Phone Services - Security Advisory - SOS-14-001

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 Spoofing Exposure of sensitive information
Attack Vector.	Remote without authentication
Solution Status.	Vendor patch Vendor workaround
CVE reference.	CVE-2014-3278 CVE-2014-3281 CVE-2014-3300
Cisco references.	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140702-cucdm http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3278 http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3281

Details.

Multiple high risk security vulnerabilities were detected in the IP phone services 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 for the IP phones 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 in the following references:

1. Cisco Unified Communications Domain Manager BVSMWeb Unauthorized Data Manipulation 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-2014-3300

A vulnerability in the web framework of the Cisco Unified Communications Domain Manager Application Software could allow an unauthenticated, remote attacker to access and modify BVSMWeb portal user information such as settings in the personal phone directory, speed dials, Single Number Reach, and call forward settings.

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

2. Cisco Unified Communications Domain Manager BVSMWeb Information Disclosure Vulnerability (Medium Risk)

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3281

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3281

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 access limited user information.

The vulnerability is due to improper implementation of authentication and authorisation controls when accessing some web pages of BVSMWeb applications. An attacker could exploit this vulnerability by submitting crafted URLs to the affected system.

3. Cisco Unified Communications Domain Manager BVSMWeb User Enumeration Vulnerability (Low Risk)

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3278

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3278

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 some web pages of the BVSMWeb application. An attacker could exploit this vulnerability by submitting crafted URLs to the affected system.

Exploits and Tools.

Viproy VoIP Penetration Testing and Exploitation Kit:

http://www.viproy.com

Solution.

All vendor security fixes must be installed. All Cisco CUCDM customers must migrate from the BVSMWeb interface of the CUCDM to the Cisco Unified Communication Manager IP telephony management services.

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-14-001.pdf

Other Sense of Security advisories can be found at:

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