

# Cisco Unity Connection – Safe Voicemail Deletion

## May 2011

Cisco Systems Inc. (Cisco) engaged iSEC Partners Inc. (iSEC) to undertake forensic assessment of the Cisco Unity Connection voicemail message deletion processes. The project involved 160 person-hours of assessment of Cisco Unity Connection version 8.5, running on a Cisco MCS 7800 series Cisco Media Convergence Server.

The testing methodology involved the following tasks being undertaken:

- Source code review around voicemail deletion processes and functions
- Black box testing and security review of the Cisco Unity Connection software
- Forensic analysis of the volatile memory and processes running on the server
- Forensic analysis of the RAID disk arrays used for persistent storage

The focus of the testing was to investigate and validated two specific security-related assertions that are made by Cisco relating to the Unity Connection software, as follows:

1. Voicemail data is processed and stored in an appropriate and safe manner
2. Voicemail data is destroyed in an appropriate and safe manner

### Assertions

iSEC security testing contains five levels of measurement. The results for each test conducted by iSEC are categorized according to the following table.

| Summary of Testing Results |       |  |
|----------------------------|-------|--|
| Measurement                | Score | Explanation                                |
| Excellent                  | 5     | Significantly exceeding industry standards |
| Good                       | 4     | Exceeding industry standards               |
| Satisfactory               | 3     | Meeting industry standards                 |
| Poor                       | 2     | Below industry standards                   |
| Bad                        | 1     | Significantly below industry standards     |

The following table summarizes the results of iSEC's testing based on Cisco's security assertions.

| Summary of Testing Results<br>Cisco Unity Connection Platform               |                     |
|---|---------------------|
| Security Assertion  | Results             |
| 1: Voicemail data is processed and stored in an appropriate and safe manner | Satisfactory<br>(3) |
| 2: Voicemail data is destroyed in an appropriate and safe manner            | Good<br>(4)         |

### Detailed Explanation of iSEC Testing & Findings

The following section lists each security assertion by Cisco, along with the iSEC testing process, and the overall results.

| Assertion 1: Voicemail data is processed and stored in an appropriate and safe manner   |
|---|
| <p><b>Testing Process:</b></p> <p>iSEC manually reviewed the Cisco Unity Connection source code functions around voicemail processing, storage, and deletion.</p> <p>iSEC then used <i>lsOf</i> to poll the operating system at regular intervals as voicemail data was being processed by the system to evaluate the way in which the software was indeed operating (black box testing).</p> <p>Finally, iSEC used EnCase 6 to forensically review three disk images that were taken: one before voicemail was left, one with voicemail data on the system, and one after voicemail data had been destroyed using the shred functionality.</p> |

**Testing Results:**

As the voicemail message is recorded, it is written to a temporary structure on disk (under /common/var-connection/spool/AudioStore/WorkStreams/) by the *CuCsMgr* process. Once the recording is complete, two copies of the message data exist on disk under /common/var-connection/, as follows:

```
[root@isececg2003 var-connection]# ls -la shredder/
total 56
drwxrwxr-x 2 root    cuservice 20480 May 19 15:36 .
drwxrwxr-x 8 root    cuservice  4096 May 18 11:20 ..
-rw-rw-r-- 1 cucsmgr cuservice 32218 May 19 15:36 cuc_3eb4af43-cfe7-4dc0-a735-115288a62974.tmp

[root@isececg2003 var-connection]# ls -la mail/unitymbxdb1/2011.05.18-18.32.41.288/
total 40
drwxrwxr-- 2 cumta  cuservice  4096 May 19 15:36 .
drwxrwxr-x 3 cumta  cuservice  4096 May 19 02:00 ..
-rw-rw-r-- 1 cumta  cuservice 32218 May 19 15:36 4d56fb24-3ef9-461b-aaa6-601750491316_1.wav
```

The temporary file is subject to shredding at 30 minute intervals, as invoked by the *CuSysAgent* process. The wave file persists on disk until it is legitimately deleted or shredded.

Forensic analysis of the disk shows that the temporary filename still persists on the disk (cuc\_3eb4af43-cfe7-4dc0-a735-115288a62974.tmp), however the content does not. The content relating to both file locations is sufficiently shredded and destroyed.

**Conclusion: Satisfactory (3)**

The Cisco Unity Connection software processes and stores voicemail data in-line with industry standards. A higher score would be awarded if these files were not world-readable by local users or processes running on the server, which is a known issue iSEC has communicated to Cisco.

Forensic analysis of the disk shows that content is irretrievable upon shredding. There may be certain edge cases where shredding fails, and it is important that the Cisco Unity Connection software operates in such a manner that if a shred failure is witnessed, the administrator is made aware of the event.

iSEC has communicated to Cisco that a way to exceed current industry standards with regard to storage and processing of sensitive materials is to use a cryptographic solution to store the data in an encrypted fashion, and destroy the keying materials upon voicemail data being marked for deletion.

**Assertion 2:** Voicemail data is destroyed in an appropriate and safe manner

**Testing Process:**

iSEC manually reviewed the source code functions around voicemail deletion.

iSEC then used *lsof* to poll the operating system at regular intervals as voicemail data was being processed and deleted by the system to evaluate the way in which the software was indeed operating (black box testing).

Finally, iSEC used EnCase 6 to forensically review three disk images that were taken: one before voicemail was left, one with voicemail data on the system, and one after voicemail data had been destroyed using the shred functionality.

**Testing Results:**

iSEC found that the shred operation (/usr/bin/shred as invoked by *CuSysAgent* every 30 minutes) performs the following for each message with a shred level of 6:

1. Open file
2. Create a buffer with 6 wipe patterns
3. Overwrite the file with the 6 patterns
4. Rename file with shorter and shorter names
5. Unlink file

The source code for this version of the RedHat Linux shred utility can be found at [http://coreutils.sourceforge.net/documentation/5.2.1/shred\\_8c-source.html](http://coreutils.sourceforge.net/documentation/5.2.1/shred_8c-source.html)

iSEC found two copies of the voicemail data on disk, at the following locations:

- cuc\_3eb4af43-cfe7-4dco-a735-115288a62974.tmp at disk location 4,999,614,646
- 4d56fb24-3ef9-461b-aaa6-601750491316\_1.wav at disk location 5,033,197,568

Using EnCase 6 to analyse the disk images from before and after shredding, iSEC verified that the data had been correctly destroyed. The screenshots from EnCase demonstrating this are attached and included with this report, as follows:

- Temp file before.png
- Temp file after.png
- Wave file before.png
- Wave file after.png

**Conclusion: Good (4)**

The Cisco Unity Connection software securely deletes wave files and material in a manner that exceeds basic industry standards.

As mentioned previously, there may be certain edge cases where shredding fails, and it is important that the Cisco Unity Connection software operates in such a manner that if a shred failure is witnessed, the administrator is made aware of the event.