# 賽門鐵克產品安全摘要報告 – 賽門鐵克解譯器引擎多重剖析漏洞 (Symantec Decomposer Engine Multiple Parsing Vulnerabilities)

## SYM16-010

**2016 年 6 月 28 日**

**重新修訂**

6/29/2016

- 防護病毒特徵已新增至賽門鐵克安全應變區段。
- 受影響產品之變更部份表格。

**嚴重程度 (CVSS v2 及 CVSS v3)**

| **CVSS**<br><br>**Base Score** | **CVSS Vector** |
|---|---|
| RAR 解壓縮記憶體存取違規 - 高 | |
| v2 7.8 | AV:N/AC:L/Au:N/C:N/I:N/A:C |

| | |
|---|---|
| v3 7.5 | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| Dec2SS 緩衝區溢位 - 高 | |
| v2 9.0 | AV:N/AC:L/Au:N/C:P/I:P/A:C |
| v3 8.6 | AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H |
| Dec2LHA 緩衝區溢位 - 高 | |
| v2 9.0 | AV:N/AC:L/Au:N/C:P/I:P/A:C |
| v3 8.6 | AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H |
| CAB 解壓縮記憶體損毀 - 高 | |
| v2 7.8 | AV:N/AC:L/Au:N/C:N/I:N/A:C |
| v3 7.5 | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| MIME 訊息修改記憶體損毀 - 高 | |

| | |
|---|---|
| v2 7.8 | AV:N/AC:L/Au:N/C:N/I:N/A:C |
| v3 7.5 | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| TNEF 整數溢位 - 低 | |
| 0.0 | AV:N/AC:L/Au:N/C:N/I:N/A:N |
| ZIP 解壓縮記憶體存取違規 | |
| v2 7.8 | AV:N/AC:L/Au:N/C:N/I:N/A:C |
| v3 7.5 | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |

**概述**

賽門鐵克在多種產品的不同組態中所使用的防毒解譯器引擎中，發現緩衝區溢位 (buffer overflow) 和記憶體損毀 (memory corruption) 漏洞。

**受影響的企業產品**

| 產品 | 版本 | 解決方案 |
| --- | --- | --- |
| Advanced Threat Protection (ATP) | | 透過病毒定義檔更新程式進行更新 |
| Symantec Data Center Security:Server (SDCS:S) | 6.0<br>6.0MP1<br>6.5<br>6.5MP1<br>6.6<br>6.6MP1 | 透過病毒定義檔更新程式進行更新 |
| Symantec Web Security .Cloud | | 透過託管型軟體更新來進行更新、客戶介面無需更新 |
| Email Security Server .Cloud (ESS) | | 透過託管型軟體更新來進行更新、客戶介面無需更新 |

| | | |
|---|---|---|
| Symantec Web Gateway | | 透過病毒定義檔更新程式進行更新 |
| Symantec Endpoint Protection (SEP) | 12.1.6 MP4 及之前版本 | 更新至 SEP 12.1 RU6 MP5 |
| Symantec Endpoint Protection for Mac (SEP for Mac) | 12.1.6 MP4 及之前版本 | 所有支援的產品版本可透過 LiveUpdate™ 進行更新 |
| Symantec Endpoint Protection for Linux (SEP for Linux) | 12.1.6 MP4 及之前版本 | 更新至 SEP for Linux<br><br>12.1 RU6 MP5 |
| Symantec Protection Engine (SPE) | 7.0.5 及之前版本 | 更新至 SPE 7.0.5 HF01<br>欲知更多詳細資訊，請參考以下知識庫連結：<br>https://support.symantec.com/en_US/article.INFO3791.html |
| | 7.5.4 及之前版本 | SPE 7.5.4 (AWS 平台) 應更新至 SPE 7.5.4 HF01<br>SPE 7.5.3 及之前版本則應更新至 SPE 7.5.3 HF03<br>欲知更多詳細資訊，請參考以下知識庫連結：<br>https://support.symantec.com/en_US/article.INFO3791.html |

| | | |
|---|---|---|
| | 7.8.0 | 更新至 SPE 7.8.0 HF01<br>欲知更多詳細資訊，請參考以下知識庫連結：<br>https://support.symantec.com/en_US/article.INFO3791.html |
| Symantec Protection for SharePoint Servers (SPSS) | 6.03 to 6.05 | 更新至 Hotfix:<br>SPSS_6.0.3_To_6.0.5_HF_1.5<br>欲知更多詳細資訊，請參考以下知識庫連結：<br>https://support.symantec.com/en_US/article.INFO3795.html |
| | 6.0.6 及之前版本 | 更新至 Hotfix:<br>SPSS_6.0.6_HF_1.6<br>欲知更多詳細資訊，請參考以下知識庫連結：<br>https://support.symantec.com/en_US/article.INFO3795.html |
| Symantec Mail Security for Microsoft Exchange . | 7.0.4 及之前版本 | 更新至 Hotfix:<br>SMSMSE_7.0_3966002_HF1.1<br>欲知更多詳細資訊，請參考以下知識庫連結：<br>https://support.symantec.com/en_US/article.INFO3794.html |
| | 7.5.4 及之前版本 | 更新至 Hotfix:<br>SMSMSE_7.5_3966008_VHF1.2<br>欲知更多詳細資訊，請參考以下知識庫連結：<br>https://support.symantec.com/en_US/article.INFO3794.html |
| Symantec Mail Security for Domino (SMSDOM) | 8.0.9 及之前版本 | 更新至 Hotfix:<br>SMSDOM_8.0.9_HF1.1<br>欲知更多詳細資訊，請參考以下知識庫連結：<br>https://support.symantec.com/en_US/article.INFO3793.html |

| | | |
|---|---|---|
| | 8.1.3 及之前版本 | 更新至 Hotfix: SMSDOM_8.1.3_HF1.2<br>欲知更多詳細資訊，請參考以下知識庫連結：<br>https://support.symantec.com/en_US/article.INFO3793.html |
| CSAPI | 10.0.4 及之前版本 | 更新至 CSAPI 10.0.4 HF01 |
| Symantec Message Gateway (SMG) | SMG 10.6.1-3 及之前版本 | 更新至 SMG 10.6.1-4 |
| Symantec Message Gateway for Service Providers (SMG-SP) | 10.6 | SMG-SP 10.6、patch 253 |
| | 10.5 | SMG-SP 10.5、patch 254 |

**受影響的諾頓產品**

| | | |
|---|---|---|
| 諾頓系列產品 | 所有 NGC 22.7 之前的版本 | 透過 LiveUpdate™ 進行更新 |
| Norton AntiVirus | | |

| | | |
|---|---|---|
| Norton Security | | |
| Norton Security with Backup | | |
| Norton Internet Security | | |
| Norton 360 | | |
| Norton Security for Mac | 所有 13.0.2 之前的版本 | |
| Norton Power Eraser (NPE) | 所有 5.1 之前的版本 | 透過 LiveUpdate™ 進行更新 |
| Norton Bootable Removal Tool (NBRT) | 所有 2016.1 之前的版本 | 最新版本已可供下載 |

**詳細資訊**

在剖析以惡意方式格式化的容器檔案時，可能會造成賽門鐵克解譯器引擎中的記憶體損毀、整數溢位或緩衝區溢位問題。成功刺探這些漏洞通常會造成應用程式層級的服務阻斷，不過也可能會造成允許執行任意程式碼。因此攻擊者有可能透過將精心設計的檔案傳送給使用者來執行任意程式碼。

在 TNEF 解除封包程式中，溢位並未因底層程式碼而產生任何有害的動作。不過，由於不恰當的建置方式，有可能在某個時間點遭到惡意人士進一步利用。因此，在解譯器引擎更新中，我們也解決了這個問題。

**賽門鐵克的應變**

賽門鐵克已確認這些問題，並根據上面我們已判斷出來的受影響產品對照表，在產品更新中解決了這些問題。我們也在我們的安全開發生命周期中新增了更多的檢查項目，以便在未來減少類似問題的發生。

賽門鐵克在外部並未發現這些漏洞受到刺探。

為了完全免除我們發現的這些漏洞，賽門鐵克建議客戶儘速對受影響的產品套用所需的修補程式。這是確保已安裝產品不會遭受攻擊的唯一方法。為了攔截/偵測攻擊者試圖進行刺探，賽門鐵克已發佈了下列病毒特徵。

| 漏洞 | 特徵 | LiveUpdate rev. |
|---|---|---|
| RAR 解壓縮記憶體存取違規 | EXP.CVE-2016-2207 | 20160628.037 |
| Dec2SS 緩衝區溢位 | EXP.CVE-2016-2209 | 20160628.037 |
| Dec2LHA 緩衝區溢位 | EXP.CVE-2016-2210 | 20160628.037 |
| CAB 解壓縮記憶體損毀 | EXP.CVE-2016-2211 | 20160628.037 |
| MIME 訊息修改記憶體損毀 | EXP.CVE-2016-3644 | 20160628.037 |
| TNEF 整數溢位 | EXP.CVE-2016-3645 | 20160628.037 |
| ZIP 解壓縮記憶體存取違規 | EXP.CVE-2016-3646 | 20160628.037 |

**更新資訊**

所有諾頓產品已透過 LiveUpdate™ 進行更新。賽門鐵克企業產品的客戶應檢查上面提供的表格，瞭解哪些產品已自動更新、哪些需要手動進行產品更新。

如何判別產品更新狀況：

| 產品 | 判別產品更新狀況 |
| --- | --- |
| Advanced Threat Protection (ATP) | 請確認已套用最新的病毒定義檔更新程式 |
| Symantec Web Security (SWS) | 請確認已套用最新的病毒定義檔更新程式 |
| Symantec Data Center Security:Server (SDCS:S) | 請確認已套用最新的病毒定義檔更新程式 |
| Symantec Endpoint Protection (SEP)<br><br>Symantec Endpoint Protection for Linux (SEP for Linux) | 所有平台 - 在「說明 -> 關於」中會反映出 MP5 版本至少為 12.1.7004.6500 |
| Symantec Endpoint Protection for Mac (SEP for Mac) | 更新後的掃描引擎版本應為 12.1.3 |
| Symantec Protection Engine (SPE) | 技術支援將會提供有關所在位置、部署及驗證步驟的通知<br><br>https://support.symantec.com/en_US/article.INFO3791.html |

| | |
|---|---|
| Symantec Protection for SharePoint Servers (SPSS) | 技術支援將會提供有關所在位置、部署及驗證步驟的通知<br><br>https://support.symantec.com/en_US/article.INFO3795.html |
| Symantec Mail Security for Microsoft Exchange . | 技術支援將會提供有關所在位置、部署及驗證步驟的通知<br><br>https://support.symantec.com/en_US/article.INFO3794.html |
| Symantec Mail Security for Domino (SMSDOM) | 技術支援將會提供有關所在位置、部署及驗證步驟的通知<br><br>https://support.symantec.com/en_US/article.INFO3793.html |
| CSAPI | 技術支援將會提供有關所在位置、部署及驗證步驟的通知 |
| Symantec Message Gateway (SMG) | 目前已安裝版本應為 10.6.1-4 |
| Symantec Message Gateway for Service Providers (SMG-SP) | 請確認已安裝的更新二進位檔案版本和修補程式發行說明中所指明的總和檢查碼 (checksum) 相同。 |

**請注意：**針對您特定的企業產品，若您需要取得更多的支援資訊，請參考：
https://support.symantec.com/en_US/article.TECH125408.html

諾頓系列產品：

產品更新會透過 LiveUpdate™ 提供。LiveUpdate™ 會定期執行，或者使用者也可自行執行互動式 LiveUpdate™。

要執行互動式 LiveUpdate™，使用者應：

- 存取產品中的 LiveUpdate™
- 執行 LiveUpdate™，直到所有可用的更新程式均已下載及安裝完成。

如已成功套用更新程式，在產品使用者介面中的「說明 -> 關於」對話框中會顯示版本為 **22.7.0.x**。

**最佳實務準則**

賽門鐵克強烈建議您採取以下一般最佳實務準則：

- 限制只有獲得授權的高權限使用者可存取系統管理用的系統。
- 限制遠端存取，如有需要，可限制只有受信任/獲得授權的系統才可進行遠端存取。
- 在最低權限的原則下執行，如此可減少可能遭受攻擊的影響。
- 利用廠商提供的修補程式將所有作業系統和應用程式維持在最新狀態。
- 遵守多層式安全方式。最少應同時執行防火牆和防惡意程式應用程式，以便針對入埠與離埠威脅提供多個偵測點與防護點。
- 部署網路或託管型入侵偵測系統，以監控網路流量，找出異常或可疑活動的徵兆。如此可協助偵測與刺探潛伏漏洞有關的攻擊或惡意活動。

**特別感謝**

賽門鐵克要特別感謝 Google Project Zero 的 Tavis Ormandy 向我們提報這些問題，並與我們密切合作以解決問題。

**參考資料**

**BID：** Security Focus http://www.securityfocus.com 已將這些問題指定 Bugtraq IDs (BIDs)，以便包含在 Security Focus 漏洞資料庫中。

**CVE：** 這些問題可能會包含在 CVE 清單中 (http://cve.mitre.org)，並將這些安全問題以標準化名稱命名。

| CVE | BID | 說明 |
|---|---|---|
| CVE-2016-2207 | 91434 | RAR 解壓縮記憶體存取違規 |
| CVE-2016-2209 | 91436 | Dec2SS 緩衝區溢位 |
| CVE-2016-2210 | 91437 | Dec2LHA 緩衝區溢位 |
| CVE-2016-2211 | 91438 | CAB 解壓縮記憶體損毀 |

| | | |
|---|---|---|
| CVE-2016-3644 | 91431 | MIME 訊息修改記憶體損毀 |
| CVE-2016-3645 | 91439 | TNEF 整數溢位 |
| CVE-2016 -3646 | 91435 | ZIP 解壓縮記憶體存取違規 |

賽門鐵克對我們的產品安全性與正常功能採取非常嚴肅的態度。身為 Organization for Internet Safety (OISafety) 的創始成員，賽門鐵克一向支持與遵守責任公開原則。
若您覺得您在賽門鐵克產品中發現任何安全問題，請連絡 secure@symantec.com。賽門鐵克產品安全團隊成員將就您提出的問題與您連絡，並協調任何所需的回應工作。有關提報漏洞的資訊，賽門鐵克強烈建議您使用加密電子郵件：secure@symantec.com。您可以在以下地點找到賽門鐵克產品安全 PGP 金鑰。
賽門鐵克已製作了一份產品漏洞回應文件，概要說明我們在解決產品中可疑漏洞時所遵循的流程。該文件可由以下連結取得。
賽門鐵克漏洞回應政策
賽門鐵克產品漏洞管理 PGP 金鑰

---



## 免責聲明

本摘要報告中的資訊是根據發佈當時我們相信正確的資訊所製作。使用本資訊即表示接受以「現狀」使用。關於此資訊，我們不提供任何保證。作者或出版者均不接受任何因使用或信賴此資訊所產生的直接、間接或衍生損失或損害的責任。

* 特徵名稱也可能已更新，以符合更新的 IPS 特徵命名規則。欲知更多資訊，請參考：http://www.symantec.com/business/support/index?page=content&id=TECH152794&key=54619&actp=LIST。
最後一次修改日期：2016 年 6 月 28 日