賽門鐵克產品安全摘要報告 — Symantec Endpoint Protection Manager 數個安全問題

SYM16-011

2016 年 6 月 28 日

重新修訂

無

嚴重程度

CVSS Base Score	CVSS2 Vector
伺服器端偽造要求身分驗證介面 - 中	
v2 4.8	AV:A/AC:M/Au:M/C:C/I:N/A:N
v3 5.4	AV:A/AC:H/PR:L/UI:R/S:C/C:H/I:N/A:N
略過身分驗證鎖定臨界值暴力破解攻擊 - 高	
v2 7.1	AV:A/AC:L/Au:S/C:C/I:C/A:N
v3 7.3	AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
洩漏 Sysadmin 已驗證清單 - 低	
v2 2.2	AV:A/AC:L/Au:M/C:P/I:N/A:N
v3 2.4	AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N
洩漏伺服器登入憑證 - 中	
v2 4.0	AV:A/AC:H/Au:M/C:C/I:N/A:N
v3 4.5	AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

SEPM 管理指令程式碼中的多個 XSS - 中	
v2 6.8	AV:A/AC:M/Au:S/C:C/I:C/A:N
v3 6.7	AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
在網頁伺服器中可存取 PHP JSESSIONID - 中	
v2 6.5	AV:A/AC:H/Au:S/C:C/I:C/A:C
v3 6.8	AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
數個 SEPM CSRF - 高	
v2 7.0	AV:A/AC:M/Au:M/C:C/I:C/A:C
v3 7.1	AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
在外部網頁 .php 指令碼中開啟重新導向 - 中	
v2 4.1	AV:A/AC:L/Au:S/C:P/I:P/A:N
v3 4.1	AV:A/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N
在 php 程序碼中操控 DOM-based 連結 - 中	
v2 5.2	AV:A/AC:M/Au:S/C:N/I:C/A:N
v3 5.2	AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
在 8445 通訊埠上未強制執行嚴格的傳輸安全規則 - 中	
v2 4.1	AV:A/AC:L/Au:S/C:P/I:P/A:N
v3 4.6	AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
管理主控台中的網頁根目錄周遊 - 中	
v2 4.1	AV:A/AC:L/Au:S/C:P/I:P/A:N

v3 4.6	AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
略過 SEP 用戶端裝置控制限制本機競爭條件 - 低	
v2 2.4 v3 2.8	AV:L/AC:H/Au:S/C:P/I:P/A:N AV:A/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N

概述

Symantec Endpoint Protection (SEP) 可能會受到幾個因使用者利用在管理主控台中提高權限或存取未經授權檔案的方式而產生的幾個安全漏洞影響。

此外，SEP 用戶端中的裝置控置競爭條件也可能允許略過安全限制，導致允許在用戶端系統上在某種程度上存取檔案下載或上傳。

受影響的產品

產品	版本	Build	解決方案
Symantec Endpoint Protection Manager 及用戶端	12.1.	全部	更新至 12.1-RU6-MP5

詳細資訊

SEP 的管理主控台 SEPM 含有數個安全漏洞，可能會遭到權限較低的使用者或未經授權的使用者利用，在管理主控台上提高權限或取得未經授權資訊的存取權限。對這些漏洞的發動刺探攻擊必須要存取 SEP 管理主控台。

介面指令碼和表單中存在的跨網站指令碼及跨網站偽造要求漏洞是用來管理主控台和產生狀態與活動報表的。管理主控台沒有提供足夠的驗證或清理傳入的輸入。它也未提供適當的 CSRF 防護。成功鎖定目標會讓未經授權或權限較低的使用者利用主控台來存取或綁架用來管理主控台的瀏覽器工作區段。如此可能會讓未經授權的使用者層級存取管理主控台，然後用來提高權限。XSS 和 CSRF 的問題都是對使用者輸入與伺服器輸出的驗證與清理功能不足所產生。在管理主控台中對這些問題發動刺探攻擊可透過欺騙已正確驗證的使用者存取精心設計的惡意連結，或透過權限較低但擁有授權的使用者在主控台上操控既有

的網址。視連結的特性而定，在被鎖定的使用者瀏覽器環境中，有可能可以執行任意 html 請求及 php 指令碼。管理主控台通常只會允許指定的使用者/系統管理員存取。

攻擊者可用伺服器端存在的偽造請求看起來像是伺服器真的在請求，以便略過現有的存取控制機制，並試圖在內部網路上掃描未經授權的內容。

具有存取 SEPM 身分驗證視窗的較低權限授權網路使用者可以略過鎖定臨界值限制，在復原有效的管理主控台密碼中進行密碼暴力破解攻擊。

擁有授權的管理主控台系統管理員可以操控 GET 物件請求，以便收集其他有效的系統管理員帳號資訊。這些資訊可能會進一步用於上面所述的使用者密碼暴力破解攻擊。

用來將產生的報表導向外部任何經授權網址的提報網址，就是可能可利用來開啟重新導向的漏洞，它能允許權限較低的授權使用者將不疑有他的高權限使用者重新導向到外部網址，以便嘗試進行進一步的刺探攻擊，例如網路釣魚。

擁有管理主控台權限的授權網路使用者可能會在既有的管理指令碼中刺探既有的 DOM 連結操控弱點 (也就是一種 XSS)，對受管理的用戶端系統發動攻擊。

SEPM 的接聽連接埠 — 8445 通訊埠上並未有效啟用 HTTP Strict Transport Security。這樣會導致資訊外洩或重新導向型的攻擊。

在管理主控台中有一個限制存取目錄周遊，它可能會讓權限較低的使用者存取網頁根目錄上的檔案/目錄。

請注意：在 Symantec Endpoint Protections 管理主控台的一般安裝中，不應該能存取網路環境外部，而內部存取則應限制特定使用者/系統管理員。在系統管理工作區段正在使用中時，授權使用者用來存取管理主控台的網頁瀏覽器絕不可用來瀏覽外部網站。這些使用限制將可大幅降低外部對這類漏洞進行攻擊的風險。

在 SEP 用戶端上，USB 隨身碟插入用戶端系統的 USB 埠和 SEP 裝置管理員對外部裝置進行存取控制之間存在一個競爭條件。在這個短暫的延遲中，擁有本地機系統存取權限的使用者就可以從用戶端系統將未經授權的敏感檔案下載至未經授權的 USB 裝置，或將任意檔案內容從外部 USB 裝置上傳至本機系統。

賽門鐵克的應變

賽門鐵克產品工程師已透過內部測試確認這些發現到的問題，並暫緩了 SEP 12.1-RU6-MP5 的發佈。賽門鐵克工程師仍繼續檢討相關功能，以便進一步強化 Symantec Endpoint Protection 的整體安全性。賽門鐵克已發佈了 Symantec Endpoint Protection 12.1 RU6 MP5，目前已可透過正常的支援管道提供給客戶。我們建議客戶儘可能立即更新至 RU6-MP5，以解決本安全摘要報告中發現的安全問題。

賽門鐵克目前並未發現客戶受到這些問題的影響。

更新資訊

您可由此取得 Symantec Endpoint Protection Manager 12.1-RU6-MP5：Symantec File Connect。

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

賽門鐵克特別感謝 Deloitte France 公司的就 CVE-2016-3647、3648、3649、3650、3651 提報資訊，並與我們共同合作解決這些問題。

賽門鐵克特別感謝 John Page (又名 hyp3rlinx) 就 CVE-2016-3652、3653 及 5304 提報資訊，並與我們共同合作解決這些問題。

賽門鐵克特別感謝 MITRE 公司的 Josh Meyer 就 CVE-2016-5304、5305、5306 和 3651 提報資訊，並與我們共同合作解決這些問題。

賽門鐵克特別感謝 MWR InfoSecurity 公司的 Che Lin Law，就 CVE-2016-5307 提報資訊，並與我們共同合作解決這些問題。

賽門鐵克特別感謝 Security Risk Advisors 的 Chris Salernofor 就 CVE-2015-8801 提報資訊給我們，並與我們共同合作解決這些問題。

參考資料

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。

BID：Symantec 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	BID	說明
CVE-2016-3647	91433	伺服器端偽造要求身分驗證介面
CVE-2016-3648	91441	略過身分驗證鎖定臨界值暴力破解攻擊
CVE-2016-3649	91440	洩漏 Sysadmin 已驗證清單
CVE-2016-3650	91432	洩漏伺服器登入憑證
CVE-2016-3651	91445	在網頁伺服器中可存取 PHP JSESSIONID
CVE-2016-3652	91444	SEPM 管理指令程式碼中的多個 XSS
CVE-2016-3653	91442	數個 SEPM CSRF
CVE-2016-5304	91447	在外部網頁 .php 指令碼中開啟重新導向
CVE-2016-5305	91448	在 php 程序碼中操控 DOM-based 連結
CVE-2016-5306	91449	在 8445 通訊埠上未強制執行嚴格的傳輸安全規則
CVE-2016-5307	91443	管理主控台中的網頁根目錄周遊
CVE-2015-8801	91446	略過 SEP 用戶端裝置控制限制本機競爭條件

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

賽門鐵克公司 2016 版權聲明

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