賽門鐵克產品安全摘要報告 – Symantec Antivirus Engine 的 PE 標頭格式錯誤剖析器記憶體存取違規

SYM16-008

2016 年 5 月 16 日

重新修訂

無

嚴重程度

嚴重程度 (CVSS v2 及 CVSS v3)

CVSS2 **Base Score**	**CVSS2 Vector**
Symantec AVE 的 PE 標頭格式錯誤剖析器記憶體存取違規 - 高	
9.4	AV:N/AC:L/Au:N/C:N/I:C/A:C

CVSS3 **Base Score**	**CVSS3 Vector**
Symantec AVE 的 PE 標頭格式錯誤剖析器記憶體存取違規 - 高	

9.1	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

概述

由於在 kernel 剖析精心設計的 PE 標頭檔案時的瑕疵，可能造成賽門鐵克的 Anti-Virus Engine (簡稱 AVE) 受到記憶體存取違規影響。成功發動攻擊最常見的徵兆是造成系統當機。

受影響的產品

產品	版本	Build	解決方案
Symantec Antivirus Engine	20151.1.0.32	全部	透過 LiveUpdate™ 更新至 Symantec Anti-Virus Engine v 20151.1.1.4

詳細資訊

賽門鐵克發現在剖析傳送到內部的格式錯誤可攜式執行 (portable-executable，簡稱 PE) 標頭檔案時，Antivirus Scan Engine 會出現一個嚴重問題。透過入埠電子郵件附件故意下載，可能會啟動精心設計格式錯誤檔案的剖析常式。
成功發動攻擊最常見的徵兆就是系統立即當機，起因是在 kernel 中的記憶體存取違規。

賽門鐵克的應變

賽門鐵克產品工程師已在最新的 AVE 更新中 (2015 年 5 月 16 日透過 LiveUpdate™ 提供給客戶的 20151.1.1.4 版)，以一般定義檔和特徵更新解決了這個問題。

更新資訊

具有預設排程 LiveUpdateTM 的諾頓安全與賽門鐵克企業產品應已接收到更新的緊急修正程式。
使用者也可按照以下步驟在互動模式中手動啟動與執行 LiveUpdate?：

- 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

賽門鐵克目前並未發現客戶受到這些問題的影響。

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，並與我們共同合作解決問題。

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-2016-2208	90653	Symantec AVE 的 PE 標頭格式錯誤剖析器記憶體存取違規

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

賽門鐵克公司 2016 版權聲明

免責聲明

* 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 16 日