本文書は**2016**年**9**月**20**日時点の英語情報の翻訳です。最新の情報は以下の**URL**より原文（英語）をご確認下さい。

https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160919_00

セキュリティアドバイザリー – シマンテックの圧縮解除のセキュリティ更新

SYM16-015

2016/09/19

概要

シマンテックは、RAR ファイル解析コンポーネントにおける 2 つの問題に対処するセキュリティ更新を公開しました。これは、複数のシマンテック製品で使われているウイルス対策の圧縮解除エンジンに存在する問題です。

悪質なフォーマットを持つ RAR コンテナファイルを解析すると、アプリケーションレベルでサービス拒否の状態が発生する可能性があります。

最も高い危険性: 中

問題の数: 2

問題点

この更新は、次の 2 つの問題に適用されます。

名称	CVE	危険性
RAR の圧縮解除でメモリが破損	CVE-2016-5310	中
RAR の圧縮解除で OOB の読み取り	CVE-2016-5309	中

影響を受ける製品

シマンテックは、この 2 つの問題を検証し、以下の製品アップデートで対処しています。

ノートン

Windows 版および Mac 版のノートン セキュリティ製品とノートン ウイルス対策製品は、LiveUpdate を通じて自動的に更新されています。

エンタープライズ

シマンテックの以下のエンタープライズ向け製品が影響を受けます。

製品名	解決策
Advanced Threat Protection: Network（ATP）	LiveUpdate を通じて自動更新
Email Security Server.Cloud（ESS）	LiveUpdate を通じて自動更新
Symantec Data Center Security: Server（DCS:S）	LiveUpdate を通じて自動更新
Symantec Endpoint Protection（SEP） Windows 版	**12.1.6 MP5:** LiveUpdate を通じて自動更新 **12.1.6 MP5 以前のバージョン:** 12.1.6 MP6 アップデートを適用し、必要に応じて再起動 詳しくは、サポート記事を参照
Symantec Endpoint Protection（SEP） Mac 版	LiveUpdate を通じて自動更新
Symantec Endpoint Protection（SEP） Linux 版	12.1.6 MP6 アップデートを適用し、必要に応じて再起動
Symantec Endpoint Protection Small Business Enterprise（SEP SBE/SEP.Cloud）	**ワークステーション:** LiveUpdate を通じて自動更新。必要に応じて再起動 **サーバー:** LiveUpdate を通じて自動更新 詳しくは、サポート記事を参照
Symantec Endpoint Protection	LiveUpdate を通じて自動更新

Cloud（SEPC）for Windows/Mac	
Symantec Endpoint Protection Small Business Edition 12.1（オンプレミスのライフサイクル終了製品）	サポート記事の指示に従う
CSAPI	10.0.4 HF02 アップデートを適用
Symantec Protection Engine（SPE）	**7.8.0:** 7.8.0 HF03 アップデートを適用 **7.5.5 およびそれ以前:** 7.5.5 HF01 アップデートを適用 **7.5.4（AWS）:** 7.5.4 HF02 アップデートを適用 **7.0.5 およびそれ以前:** SPE 7.0.5 HF02 アップデートを適用 詳しくは、サポート記事を参照
Symantec Mail Security for Domino（SMSDOM）	**8.1.3:** SMSDOM_8.1.3_HF2.2 アップデートを適用 **8.1.2:** SMSDOM_8.1.2_HF2.3 アップデートを適用 **8.0.9 およびそれ以前:** SMSDOM_8.0.9_HF2.1 アップデートを適用 詳しくは、サポート記事を参照
Symantec Mail Security for Microsoft Exchang（SMSMSE）	**7.5.4 およびそれ以前:** SMSMSE_7.5_3966008_VHF2.2 アップデートを適用 **7.0.4 およびそれ以前:** SMSMSE_7.0_3966002_HF2.1 アップデートを適用 **6.5.8:** SMSMSE_6.5.8_3968140_HF2.3 アップデートを適用

	詳しくは、サポート記事を参照
Symantec Protection for SharePoint Servers (SPSS)	**6.0.7**: SPSS_6.0.7_HF_2.7 アップデートを適用 **6.0.6**: SPSS_6.0.6_HF_2.6 アップデートを適用 **6.0.3 から 6.0.5**: SPSS_6.0.3_To_6.0.5_HF_2.5 アップデートを適用 詳しくは、サポート記事を参照
Symantec Message Gateway (SMG)	SMG 10.6.2 アップデートを適用
Symantec Message Gateway for Service Providers (SMG-SP)	**10.6**: SMG-SP 10.6 patch 259 アップデートを適用 **10.5**: SMG-SP 10.5 patch 260 アップデートを適用
Symantec Web Gateway	LiveUpdate を通じて自動更新
Symantec Web Security Service.Cloud (WSS)	LiveUpdate を通じて自動更新

問題の詳細

RAR の圧縮解除でメモリが破損

CVE-2016-5310

BID: 92866

危険性: 中 (CVSSv3: 6.9) - AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

影響: サービス拒否

悪用: なし

パッチ公開日: 2016/9/16

悪質なフォーマットの RAR コンテナファイルを解析すると、メモリ破損が発生する可能性があります。これによって、アプリケーションレベルでサービス拒否の状態が発生しますが、それ以上の悪用の恐れはありません。

RAR の圧縮解除で OOB の読み取り

CVE-2016-5309

BID: 92868

危険性: 中（CVSSv3: 4.8）- AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

影響: サービス拒否

悪用: なし

パッチ公開日: 2016/9/16

悪質なフォーマットの RAR コンテナファイルを解析すると、境界外（OOB）読み取りエラーが発生する可能性があります。これによって、アプリケーションレベルでサービス拒否の状態が発生しますが、それ以上の悪用の恐れはありません。

ベストプラクティス

攻撃を受けるリスクを緩和するために、以下の対策をとることをお勧めします。

- 管理システムまたは統御システムへのアクセスを、特権ユーザーに限定します。
- リモートアクセスを信頼できるシステムや認証されたシステムのみに制限します。
- 可能な限り最小の権限を付与する原則の下で操作を実行し、脅威による悪用の影響を制限します。
- すべてのオペレーティングシステムとアプリケーションにベンダーが提供する最新の修正プログラムを適用することにより、常に最新の状態にしておきます。
- 多重的なセキュリティ対策を講じます。少なくともファイアウォールおよびマルウェア対策アプリケーションを実行し、システムに侵入および流出する脅威を複数の場所で検出および防止します。
- ネットワークおよびホストベースの侵入検知システムを導入し、ネットワークトラフィック上で異常な、または不審なアクティビティの兆候がないかどうかを監視します。これにより、潜在的な脆弱性の悪用を試みる攻撃の検知、およびそのような攻撃が成功した場合に発生する不正行為の検出が可能になります。

謝辞

Google Project Zero の Tavis Ormandy 氏（CVE-2016-5309、CVE-2016-5310）

改定履歴

なし

シマンテックでは弊社製品のセキュリティと適切な機能を重要視しています。Organization for Internet Safety（OISafety）の設立メンバーとして、シマンテックは責任ある開示方針を支持し、従っています。また、シマンテックは NIAC（National Infrastructure Advisory Council: 米国の国家インフラ諮問委員会）によりまとめられた脆弱性公開ガイドラインに賛同しています。

シマンテック製品のセキュリティ上の問題を発見した場合は、secure@symantec.com までご連絡ください。シマンテック製品セキュリティチームの担当者が、折り返しご連絡させていただきます。secure@symantec.com に脆弱性情報を報告する際は、暗号化された電子メールを使用することを強くお勧めします。シマンテック製品のセキュリティ PGP キーはこのメッセージの末尾にあります。

シマンテックでは弊社製品に存在する疑いがある脆弱性への対応プロセスについて概説した、シマンテック製品の脆弱性への対応ドキュメントを作成しました。このドキュメントは次の場所から入手できます。

シマンテック製品の脆弱性への対応ポリシー

PGP シマンテック製品の脆弱性管理 PGP キー

免責事項

＊ シグネチャ名は IPS シグネチャ命名規則の更新に準じて更新されている場合があります。詳しくは、http://www.symantec.com/business/support/index?page=content&id=TECH152794&key=54619&actp=LIST を参照してください。

最終修正日: 2016/9/16