本文書は 2016 年 6 月 30 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=20160628_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エンジンの解析に複数の脆弱性

SYM16-010

2016/06/28
改定履歴

2016/06/29

- 「弊社の対応」に保護シグネチャを追加しました。
- 影響を受ける製品の表を更新しました。

危険性（CVSS v2 と CVSS v3）

CVSS 基本値	CVSS 基本区分
RAR の圧縮解除にメモリアクセス違反 - 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 のバッファオーバーフロー - 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 のバッファオーバーフロー - 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 の圧縮解除でメモリが破損 - 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 メッセージの変更でメモリが破損 - 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 の整数オーバーフロー - 低	
0.0	AV:N/AC:L/Au:N/C:N/I:N/A:N
ZIP の圧縮解除にメモリアクセス違反	
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

概要

複数のシマンテック製品によってさまざまな構成で使われているウイルス対策の圧縮解除エンジンに、バッファオーバーフローとメモリ破損が見つかっていることをシマンテックは確認しています。

影響を受けるエンタープライズ製品

製品名	バージョン	解決策
Advanced Threat Protection（ATP）		定義更新ファイルで更新済み
Symantec Data Center Security:Server（SDCS:S）	6.0 6.0MP1 6.5 6.5MP1 6.6 6.6MP1	定義更新ファイルで更新済み
Symantec Web Security .Cloud		ホスティング型ソフトウェア更新で更新済み。ユーザーの操作は不要
Email Security Server .Cloud（ESS）		ホスティング型ソフトウェア更新で更新済み。ユーザーの操作は不要
Symantec Web Gateway		定義更新ファイルで更新済み

Symantec Endpoint Protection（SEP）	12.1.6 MP4 およびそれ以前	SEP 12.1 RU6 MP5 に更新する
Symantec Endpoint Protection for Mac（SEP for Mac）	12.1.6 MP4 およびそれ以前	サポート対象のバージョンの製品はすべて、LiveUpdate™ を通じて更新済み
Symantec Endpoint Protection for Linux（SEP for Linux）	12.1.6 MP4 およびそれ以前	SEP for Linux 12.1 RU6 MP5 に更新する
Symantec Protection Engine（SPE）	7.0.5 およびそれ以前	SPE 7.0.5 HF01 に更新する 詳しくは、次の KB リンクを参照: https://support.symantec.com/en_US/article.INFO3791.html
	7.5.4 およびそれ以前	SPE 7.5.4（AWS プラットフォーム）は、SPE 7.5.4 HF01 に更新する SPE 7.5.3 およびそれ以前のバージョンは、SPE 7.5.3 HF03 に更新する 詳しくは、次の KB リンクを参照: https://support.symantec.com/en_US/article.INFO3791.html
	7.8.0	SPE 7.8.0 HF01 に更新する 詳しくは、次の KB リンクを参照: https://support.symantec.com/en_US/article.INFO3791.html
Symantec Protection for SharePoint Servers（SPSS）	6.03 ～ 6.05	次のホットフィックスに更新する: SPSS_6.0.3_To_6.0.5_HF_1.5 詳しくは、次の KB リンクを参照: https://support.symantec.com/en_US/article.INFO3795.html
	6.0.6 およびそれ以前	次のホットフィックスに更新する: SPSS_6.0.6_HF_1.6 詳しくは、次の KB リンクを参照: https://support.symantec.com/en_US/article.INFO3795.html
Symantec Mail Security for Microsoft Exchange（SMSMSE）	7.0.4 およびそれ以前	次のホットフィックスに更新する: SMSMSE_7.0_3966002_HF1.1 詳しくは、次の KB リンクを参照: https://support.symantec.com/en_US/article.INFO3794.html
	7.5.4 およびそれ以前	次のホットフィックスに更新する: SMSMSE_7.5_3966008_VHF1.2 詳しくは、次の KB リンクを参照: https://support.symantec.com/en_US/article.INFO3794.html

Symantec Mail Security for Domino（SMSDOM）	8.0.9 およびそれ以前	次のホットフィックスに更新する: SMSDOM_8.0.9_HF1.1 詳しくは、次の KB リンクを参照: https://support.symantec.com/en_US/article.INFO3793.html
	8.1.3 およびそれ以前	次のホットフィックスに更新する: SMSDOM_8.1.3_HF1.2 詳しくは、次の KB リンクを参照: https://support.symantec.com/en_US/article.INFO3793.html
CSAPI	10.0.4 およびそれ以前	CSAPI 10.0.4 HF01 に更新する
Symantec Message Gateway（SMG）	SMG 10.6.1-3 およびそれ以前	SMG 10.6.1-4 に更新する
Symantec Message Gateway for Service Providers（SMG-SP）	10.6	SMG-SP 10.6、パッチ 253
	10.5	SMG-SP 10.5、パッチ 254

影響を受けるノートン製品

ノートン製品ファミリー	NGC 22.7 以前のすべて	LiveUpdate™ を通じて更新済み
ノートン アンチウイルス		
ノートン セキュリティ		
ノートン セキュリティ with バックアップ		
ノートン インターネットセキュリティ		
ノートン 360		
ノートン セキュリティ Mac 版	13.0.2 以前のすべて	
ノートン パワーイレイサー（NPE）	5.1 以前のすべて	LiveUpdate™ を通じて更新済み
Norton Bootable Removal Tool（NBRT）	2016.1 以前のすべて	新しいリリースをダウンロード可能

解説

悪質な形式のコンテナファイルを解析すると、シマンテックの圧縮解除エンジンでメモリ破損、整数オーバーフロー、またはバッファオーバーフローが起きることがあります。これらの脆弱性が悪用されると、一般的にはアプリケーションレベルでサービス拒否が起きますが、任意のコードが実行されることも考えられます。可能性として、攻撃者は特別に細工したファイルをユーザーに送り付けることで、任意のコードを実行できます。

圧縮解除ツール TNEF では、オーバーフローが発生しても、基盤になるコードが原因で有害な処理が行われることはありません。しかし、これは不適切な実装による無防備状態なので、悪質なユーザーによって今後さらに悪用される恐れもあります。したがって、この点もエンジンの更新で対処されました。

弊社の対応
弊社でもこれらの問題は確認済みであり、影響を受ける製品の表で「解決策」の項に記したとおり、製品の更新版で対処しました。今後の類似した問題を低減するために、Secure Development LifeCycle にチェックも追加しました。

これらの脆弱性の悪用による被害が実際に確認されたという報告はまだありません。

確認された脆弱性に完全対処するために、影響を受ける製品についてはできるだけ速やかにパッチを適用することをお勧めします。それが、インストール済みの製品を悪用されないようにする唯一の確実な手段です。シマンテックは、悪用の試みを遮断/検出するために、以下のリストのシグネチャをリリースしました。

脆弱性	シグネチャ	LiveUpdate のリビジョン
RAR の圧縮解除にメモリアクセス違反	EXP.CVE-2016-2207	20160628.037
Dec2SS のバッファオーバーフロー	EXP.CVE-2016-2209	20160628.037
Dec2LHA のバッファオーバーフロー	EXP.CVE-2016-2210	20160628.037
CAB の圧縮解除でメモリが破損	EXP.CVE-2016-2211	20160628.037
MIME メッセージの変更でメモリが破損	EXP.CVE-2016-3644	20160628.037
TNEF の整数オーバーフロー	EXP.CVE-2016-3645	20160628.037
ZIP の圧縮解除にメモリアクセス違反	EXP.CVE-2016-3646	20160628.037

更新情報
ノートン製品はすべて、LiveUpdate™ を通じて更新済みです。シマンテックエンタープライズ製品をお使いのお客様は、以下の表を確認して、自動更新済みの製品と、更新が必要な製品をお確かめください。

製品更新の確認

製品名	製品更新の確認
Advanced Threat Protection（ATP）	最新の定義ファイルが更新されていることを確認する
Symantec Web Security（SWS）	最新の定義ファイルが更新されていることを確認する
Symantec Data Center Security:Server（SDCS:S）	最新の定義ファイルが更新されていることを確認する

Symantec Endpoint Protection（SEP） Symantec Endpoint Protection for Linux（SEP for Linux）	[all platforms - Help]->[About]を選択し、MP5 のリリースバージョンが 12.1.7004.6500 以上であることを確認する
Symantec Endpoint Protection for Mac（SEP for Mac）	更新後のスキャンエンジンが、バージョン 12.1.3 であることを確認する
Symantec Protection Engine（SPE）	場所、配布、検証の手順については、サポートから通知がある https://support.symantec.com/en_US/article.INFO3791.html
Symantec Protection for SharePoint Servers（SPSS）	場所、配布、検証の手順については、サポートから通知がある https://support.symantec.com/en_US/article.INFO3795.html
Symantec Mail Security for Microsoft Exchange（SMSMSE）	場所、配布、検証の手順については、サポートから通知がある https://support.symantec.com/en_US/article.INFO3794.html
Symantec Mail Security for Domino（SMSDOM）	場所、配布、検証の手順については、サポートから通知がある https://support.symantec.com/en_US/article.INFO3793.html
CSAPI	場所、配布、検証の手順については、サポートから通知がある
Symantec Message Gateway（SMG）	現在インストールされているバージョンが 10.6.1-4 であることを確認する
Symantec Message Gateway for Service Providers（SMG-SP）	更新後のバイナリのインストール済みバージョンで、チェックサムがパッチのリリースノートで指定されているものと同じあることを確認する

注意: お使いのエンタープライズ製品について、サポート情報の入手先など詳しくは https://support.symantec.com/en_US/article.TECH125408.html を参照してください。

ノートンファミリー:

製品の更新版は、LiveUpdate™ を通じて配信されます。LiveUpdate™ は定期的に実行されますが、ユーザーがインタラクティブに LiveUpdate™ を実行することもできます。

LiveUpdateTM をインタラクティブに実行する方法は、次のとおりです。

- 製品で LiveUpdateTM にアクセスします。
- 利用可能な更新がすべてダウンロードされインストールされるまで、LiveUpdate™ を実行します。

更新が正常に適用されれば、製品 UI の[Help]->[About]にバージョンが**「22.7.0.x」**と表示されます。

ベストプラクティス

通常のベストプラクティスの一環として、以下のことを強く推奨します。

- 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。
- 必要に応じて、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。

クレジット

これらの問題をご報告いただき、問題解決にご協力いただいた Google Project Zero の Tavis Ormandy 氏に感謝いたします。

参考情報

BID: Security Focus（http://www.securityfocus.com）は、SecurityFocus 脆弱性データベースに登録するために、これらの問題に Bugtraq ID (BID) を割り当てました。

CVE: これらの問題は、さまざまなセキュリティ問題の名称が標準化されている CVE（Common Vulnerabilities and Exposures）リスト（http://cve.mitre.org/cve）への登録候補となっています。

CVE	BID	解説
CVE-2016-2207	91434	RAR の圧縮解除にメモリアクセス違反
CVE-2016-2209	91436	Dec2SS のバッファオーバーフロー
CVE-2016-2210	91437	Dec2LHA のバッファオーバーフロー
CVE-2016-2211	91438	CAB の圧縮解除でメモリが破損
CVE-2016-3644	91431	MIME メッセージの変更でメモリが破損
CVE-2016-3645	91439	TNEF の整数オーバーフロー
CVE-2016 -3646	91435	ZIP の圧縮解除にメモリアクセス違反

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

シマンテック製品の脆弱性管理 PGP キー

免責事項
本サイトの記載情報は、公開時点で確認されていた情報を基に正確であると判断された内容で構成されています。本サイトの記載情報の使用は、現状のままとすることを条件に認められています。本サイトの記載内容について、シマンテックは一切保証しないものとします。また、本サイトの記載情報の使用あるいは信頼性に関連して生じる直接的、間接的、派生的な損失または損害に関して、本サイトの著者も発行者も一切責任を負わないものとします。

* 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: 2016/06/28