ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●圧縮ファイル関連の脆弱性「Zip Slip」、大手プロジェクト多数に影響

http://www.itmedia.co.jp/enterprise/articles/1806/06/news061.html
https://forest.watch.impress.co.jp/docs/news/1126064.html

このニュースをザックリ言うと･･･

- 6月5日（現地時間）、イギリスのセキュリティベンダーSnyk Security社より、圧縮ファイルを処理する「アーカイバー」の多くに存在するとされる脆弱性「Zip Slip」について警告が出されました。

- 「../../evil.sh」といった不正な展開先が指定された圧縮ファイルを展開することにより、想定外の外部ディレクトリ上にファイルが展開され、最悪の場合、リモートから任意のコードの実行が可能になるとされています。

- 脆弱性があるとされるソフトウェアは特にJavaで顕著とされ、JavaScript・.NET等でも確認されており、影響を受ける圧縮ファイル形式も「zip」だけでなく、「tar」「jar」「war」「cpio」「apk」「rar」「7z」等があるとのことです。

AUS便りからの所感等

- 圧縮ファイルの展開によって、通常はユーザに気付かれないまま、外部ディレクトリに不正なファイルが置かれたり、実行ファイルや設定ファイルが上書きされることがこの脆弱性の肝となっています。

- 本来想定されない外部のディレクトリ上のファイルを参照したりする脆弱性は「ディレクトリトラバーサル」と呼ばれ、様々なアプリケーションで古くから知られている脆弱性です。

- アーカイバーにおいてもこういった脆弱性が存在し得ることが指摘され、著名なアプリケーションでは修正されてきたはずですが、Java等のライブラリにおいては未対策の状態が続いていた模様です。

- こういった脆弱性を突く不正な展開先を持つ圧縮ファイルは特徴的とみられ、アンチウイルスやUTMのパターンファイルでマルウェア同様に扱われていくことが期待されますので、くれぐれもアンチウイルス等による防御を確実に行い、不審な圧縮ファイルを受け取ったとしても安易に展開しないよう注意を払いましょう。

ITmedia エンタープライズ

アーカイブファイル関連の脆弱性「Zip Slip」、大手プロジェクト多数に影響

セキュリティ企業Snykによると、Zip Slipの脆弱性は、HPやAmazon、Apache、Pivotalなどを含め、数千ものプロジェクトに影響を及ぼすという。

2018年06月06日 08時30分 公開　[鈴木聖子，ITmedia]

印刷　通知　145　116　B! 46

オープンソース製品のセキュリティ対策を手掛けるSnyk Securityは6月5日、アーカイブファイルの処理に関連して、多数のオープンソースプロジェクトに影響を及ぼす重大な脆弱性を発見したと発表した。

同社はこの脆弱性

Snykによると、Zip Slipの脆弱性は、JavaScript、Ruby、.NET、Goといった複数のエコシステムで発見され、特にJavaで顕証していることが判明した。「tar」「jar」「war」「cpio」「apk」「rar」「7z」など、膨大な数のアーカイブフォーマットが影響を受けるという。

細工を施したアーカイブを使ってこの脆弱性を悪用されれば、任意のファイルが上書きされ、リモートでコマンドを実行される恐れがあるとしている。

Snykでは2018年の4月から5月にかけて、影響を受けるベンダーやプロジェクトチームに連絡を取ったという。これを受けて、Apache Hadoop、HPのFortify Cloud Scan Jenkins Plugin、AmazonのAWS Toolkit for Eclipseなど、多数の製品やサービスで脆弱性が修正されている。

Snykはこうしたライブラリを使っている組織などに対し、自分たちのプロジェクトでZip Slipの脆弱性があるコードを使っているかどうかチェックして、脆弱性を修正したバージョンのライブラリが使われていることを確認するよう呼び掛けている。

窓の杜 WINDOWS FOREST

広く採用されている書庫展開処理に任意コード実行を許す脆弱性 ～数千のプロジェクトに影響

英セキュリティ企業が"Zip Slip"と命名、StackOverflowを介して拡散か

樽井 秀人　2018年6月6日 16:00

ツイート リスト　いいね！52　シェア　B! 49　Pocket 63

イギリスのセキュリティベンダーSnykは5日（現地時間）、多くのオープンソースプロジェクトやライブラリで広く採用されている書庫ファイルの展開処理に重大な脆弱性があることを明らかにした。この脆弱性は"Zip Slip"と命名されており、リモートから任意のコードを実行可能になるという。

同社によると、書庫

"Zip Slip"脆弱性の影響を受けるプロジェクトは、JavaScript、Ruby、.NET、Goなど、プラットフォームを問わず確認されているが、なかでもプログラミング言語のコアライブラリで高水準なアーカイブ処理を提供していないJavaで顕著にみられるとのこと。開発者向けのQ&Aサイト"StackOverflow"などを介して脆弱性のあるコードスニペット（ソースコードの断片、サンプル）が共有され、そのまま使われていたようだ。

本脆弱性は4月半ばに報告され、非公開でHP、Amazon、Apache、Pivotalなどのベンダーへ通知された。大半のプロジェクトではすでに対策が実施されており、最新版へ更新すれば問題は解決される。影響を受ける製品とバージョン、対策の有無などは"GitHub"のプロジェクトページでまとめられている。

●WordPressやJoomlaを利用する5000超Webサイト、PHPマルウェア「Brain Food」に感染

https://news.mynavi.jp/article/20180525-634986/

このニュースをザックリ言うと・・・

- 5月18日（現地時間）、メールセキュリティベンダーのProofpoint社より、過去4ヶ月で5000以上のサイトに感染しているマルウェア「Brain Food」について警告が出されています。

- Brain FoodはPHPで開発され、ボットネットを構成するマルウェアとされており、WordPressやJoomlaといったPHP製のCMSで構築されたWebサイトに感染するとされています。

- ダイエットサプリやスマートドラッグの販売を行うサイトへ被害者を誘導するスパムメールを送信することからBrain Foodと名付けられている模様で、メールには件名がなく、短い挨拶文のあとに短縮URLが掲載されているだけという特徴があるとされています。

AUS便りからの所感等

- Brain Foodがどういった経路からWebサイトに感染するかは現時点で詳しい情報がないようですが、これまで報告されている古いバージョンの脆弱性を突いてWebサイトの改ざんを行っていると考えるのが自然でしょう。

- とにかく根本的な対策として、CMSやPHPその他Webサーバ上の各種ソフトウェアにすべてのセキュリティパッチを適用することが重要であり、併せて、不正なリクエストを遮断するためにサーバ上等にWAFを設置することや、内部から不正なメールを送信されないような出口対策をとることも検討するのが良いでしょう。


マイナビニュース

2018/05/25 09:30:49 印刷

5000超Webサイト、PHPマルウェア「Brain Food」に感染

後藤大地

関連キーワード：マルウェア，サイバー攻撃

WordPressやJoomlaといったCMSを運用している場合、「Brain Food」と呼ばれるPHPベースのマルウェアに感染していないかどうか調べたほうがよいかもしれない。Proofpointはこのほど「Brain Food botnet gives website operators heartburn | Proofpoint」において、過去4カ月で5000以上のサイトがBrain Foodに感染していることを発見したと伝えている。

「Brain Food」はPHPを使って開発されたボットネット・マルウェア。ダイエットサプリやスマートドラッグの販売を行うサイトへ被害者を誘導し、拡散は短縮URLを含んだシンプルなメールを送信するというスパムキャンペーンが使われているという。メールにはタイトルがなく、短い挨拶文のあとに短縮URLが掲載されている。

●Flash Playerの脆弱性を突く攻撃発生…臨時アップデート30.0.0.113で対処

http://www.itmedia.co.jp/enterprise/articles/1806/08/news066.html

このニュースをザックリ言うと・・・

- 6月7日（現地時間）、Adobe社より、Flash Playerの最新バージョン30.0.0.113がリリースされました。

- 前のバージョンである29.0.0.171までに存在している4件の脆弱性が修正されており、既にその脆弱性を悪用する不正なFlashコンテンツを埋め込んだOffice文書をメールで送りつける攻撃が確認されていることから、Adobe社でも直ちに最新バージョンへのアップデートを呼び掛けています。

AUS便りからの所感等

- Flash Playerの脆弱性は毎月のように報告・修正されており、最新バージョンにアップデートしていないPCに感染するランサムウェア等のマルウェアも存在し（「AUS便り 2018/06/04号」参照）、さらには修正前の脆弱性が悪用されるケースも珍しくありません。

- 通常であれば自動的に最新バージョンにアップデートされますが、確認ページ（https://get.adobe.com/jp/flashplayer/about/）等で確認するのが良いでしょう。

- Windows8以降のIEやWindows10のEdge向けのFlash Playerは少々遅れてWindows Updateにより リリースされます。

- 最新バージョンへのアップデートに間に合わない等のケースにおいて、未修正の脆弱性を突かれる可能性を軽減するため、アンチウイルスやUTMによる防御を普段から必ず行い、今日ではブラウザ側で一般的でないFlashコンテンツの実行時に確認を求める等の機能がありますが、場合によってはFlash機能自体を無効化する設定も考慮に値するでしょう。


ITmedia エンタープライズ

Flash Playerの脆弱性を突く攻撃発生、臨時アップデートで対処

脆弱性を突く攻撃の発生が確認されていることから、最優先で対応するよう呼び掛けている。

2018年06月08日 09時55分 公開 [鈴木聖子，ITmedia]

印刷 通知 25 4 B! 1

米Adobe Systemsは6月7日、Flash Playerの深刻な脆弱性を修正する臨時セキュリティアップデートを公開した。脆弱性を突く攻撃の発生が確認されていることから、最優先で対応するよう呼び掛けている。

Adobeのセキュリティ情報によると、今回のアップデートでは、「Flash Player 29.0.0.171」までのバージョンに存在する4件の脆弱性を修正した。うち2件については任意のコード実行に利用される恐れがあり、緊急度は同社の3段階評価で最も高い「クリティカル」に指定している。

Vulnerability Category	Vulnerability Impact	Severity	CVE Number
Type Confusion	Arbitrary Code Execution	Critical	CVE-2018-4945
Integer Overflow	Information Disclosure	Important	CVE-2018-5000
Out-of-bounds read	Information Disclosure	Important	CVE-2018-5001
Stack-based buffer overflow	Arbitrary Code Execution	Critical	CVE-2018-5002

今回アップデートで修正された4つの脆弱性（出典：Adobe）