— AUS（アルテミス・ユーザ・サポート）便り 2019/09/30号 —
https://www.artemis-jp.com

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。

●IEに「緊急」の脆弱性、リモートから任意のコードを実行される恐れ

https://internet.watch.impress.co.jp/docs/news/1208912.html
https://www.itmedia.co.jp/news/articles/1909/24/news088.html
https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2019-1367

このニュースをザックリ言うと･･･

- 9月24日(日本時間)、マイクロソフト(以下、MS)より、Internet Explorer(以下IE)の脆弱性(CVE-2019-1367)を修正するセキュリティパッチがリリースされました。
- 脆弱性はIEのスクリプトエンジンに存在するもので、IEによる不正なWebページの閲覧等により、悪用される可能性があるとみられます。
- MSでは既に脆弱性を悪用する攻撃を確認しており、速やかなパッチの適用を呼び掛けています。

AUS便りからの所感等

- 脆弱性の悪用により、Windowsにログオンしているユーザーの権限で任意のコードを実行される恐れがあり、特に管理者としてログオンしている場合、プログラムのインストールや不正なアカウントの作成等が可能とされています。
- セキュリティパッチは9月25日時点でWindows Updateでは配布されておらず(※)、上記MSのページ内のダウンロードリンクを経由してMicrosoft Updateカタログから入手し、手動でインストールする必要があるかもしれません(この場合、使用しているWindowsのバージョンに合ったパッチファイルをダウンロードすること、およびWindows 7の場合はIE11がインストールされている必要があることに注意してください)。
- 脆弱性の根本的な対策を考えるならば、手動であってもセキュリティパッチを適用することが最も重要ですが、パッチの適用が間に合わない段階で攻撃を受ける可能性もあり、これを緩和するためにも、アンチウイルスやUTMによる防御の併用は是非とも行うべきです。


INTERNET Watch

INTERNET Watch 〉 トピック 〉 セキュリティ 〉 脆弱性/修正パッチ

ニュース

IEに"緊急"の脆弱性、リモートから任意のコードを実行される恐れ

磯谷 智仁　2019年9月24日 16:53

ツイート リスト　いいね！ 88　シェア　B! 27　Pocket 7

CVE-2019-1367 | スクリプト エンジンのメモリ破損の脆弱性
セキュリティ上の脆弱性

Microsoftは、Internet Explorer（IE）にリモートから任意のコードを実行される脆弱性（CVE-2019-1367）が存在することを明らかにした。すでにこの脆弱性を悪用した攻撃が確認されているという。

IEのスクリプトエンジンにメモリ破損の脆弱性が存在しており、同脆弱性を悪用すると、攻撃者にユーザー権限を取得される恐れがある。もし、ユーザーが管理者権限でログオンしている場合は、攻撃者によりプログラムのインストールや、データの表示、変更、削除、完全なユーザー権限を持つ新たなアカウントを作成される可能性がある。

ウェブベースでの攻撃シナリオとしては、細工を施したウェブサイトでURLを表示するようにユーザーを誘導することなどが想定される。


Microsoft | MSRC

セキュリティ更新プログラム ガイド > 詳細

CVE-2019-1367 | スクリプト エンジンのメモリ破損の脆弱性

セキュリティ上の脆弱性

公開日: 2019/09/23
MITRE CVE-2019-1367

スクリプト エンジンが Internet Explorer でメモリ内のオブジェクトを処理する方法に、リモートでコードが実行される脆弱性が存在します。この脆弱性により、攻撃者が現在のユーザーのコンテキストで任意のコードを実行できるように、メモリを破損させる可能性があります。攻撃者によりこの脆弱性が悪用された場合、攻撃者が現在のユーザーと同じユーザー権限を取得する可能性があります。現在のユーザーが管理者ユーザー権限でログオンしているときに、攻撃者によりこれらの脆弱性が悪用された場合、影響を受けるコンピューターが制御される可能性があります。攻撃者は、その後、プログラムのインストール、データの表示、変更、削除などを行ったり、完全なユーザー権限を持つ新たなアカウントを作成したりする可能性があります。

Web ベースの攻撃シナリオでは、攻撃者は Internet Explorer を介して この脆弱性を悪用することを目的として特別に細工した Web サイトをホストし、メールを送信するなどして、その Web サイトを表示するようにユーザーを誘導する可能性があります。

このセキュリティ更新プログラムは、スクリプト エンジンがメモリ内のオブジェクトを処理する方法を変更することにより、これらの脆弱性を解決します。

このページのトピック
概要
悪用可能性指標
ソフトウェア更新
問題を緩和する要素
回避策
よく寄せられる質問
謝辞
免責
更新履歴

悪用可能性指標

以下の表には、この脆弱性に対する公開時の悪用可能性指標を示しています。

一般に公開	悪用	最新のソフトウェア リリース	過去のソフトウェア リリース	サービス拒否
なし	あり	0 - 悪用の事実を確認済み	0 - 悪用の事実を確認済み	対象外

※9月30日現在、Windows10ではセキュリティパッチを含むより新しい更新プログラムがWindows Updateで入手可能になっています。

●2019年上半期のマルウェアレポートを公開…キヤノンマーケティングジャパン

https://internet.watch.impress.co.jp/docs/news/1208342.html
https://eset-info.canon-its.jp/malware_info/trend/detail/190920.html

このニュースをザックリ言うと・・・

- 9月20日(日本時間)、ESET社のセキュリティ製品を国内で販売しているキヤノンマーケティングジャパン社(以下、キヤノンMJ)より、ESET社製品が2019年上半期(1～6月)に検出したマルウェアの動向をまとめた「マルウェアレポート」が発表されました。

- 国内で検出されたマルウェアで最も多かったのは「JS/Danger.ScriptAttachment(メールに添付された悪意あるJavaScriptファイルの汎用検出名)」で全体の12.3%を占めており、これについて「2018年にはほとんど観測されていなかったが、今年1月以降多数の攻撃が確認されている」「日本の芸能人名をメールの件名に入れたものが多数あり、日本のユーザーを狙った攻撃と考えられる」としています。

- この他にも「JS/Adware.Agent(ブラウザー上で不正な広告を表示するJavaScriptプログラム)」や「VBA/TrojanDownloader.Agent(Word・Excel形式の、VBAで作成されたダウンローダー)」といったマルウェアが上位に入る等、JavaScript形式・VBA形式のファイルが添付されたメールを媒介とした攻撃が多かったとされています。

AUS便りからの所感

- 同レポートでは前述したマルウェア検出統計以外にもいくつかのトピックに言及しており、例えば昨年より国内で猛威を振るったランサムウェア「GandCrab」の開発者が6月に提供の停止を宣言したことを取り上げている一方で、他のランサムウェアの発生も引き続き確認しているとしています。

- 全世界や日本国内でどういったマルウェアが拡散しているかの傾向の他に、マルウェアに対し改めてユーザーがとるべき対策のヒントも多く掲載されていますので、他社による同様のレポートも含め、随時情報収集を行い、UTMをはじめとしたセキュリティ製品導入等の検討材料として頂ければ幸いです。

●ローソン、攻撃により公式サイトとアプリを一時停止…現在は復旧

https://n1ab.itmedia.co.jp/n1/articles/1909/25/news068.html
https://n1ab.itmedia.co.jp/n1/articles/1909/26/news067.html
http://lawson.co.jp/company/news/detail/1387767_2504.html

このニュースをザックリ言うと・・・

- 9月25日(日本時間)、ローソンより、同社Webサーバーおよびスマホアプリ用サーバーが攻撃を受けたことにより、一時的にアクセスを遮断したと発表されました。

- 発表によれば、同24日20時頃に攻撃を確認しており、その後防御策を講じ、同26日5時30分にはサービスが再開されています。

- 現時点では利用者への直接的な影響や個人情報の流出は確認されておらず、引き続き外部の専門機関にも依頼して調査するとしています。

AUS便りからの所感等

- 今回発生した攻撃が、例えばDDoS攻撃だったのか、あるいは個人情報を狙ったものとみられるのかといった詳細は現時点で不明ですが、Webサイトの閲覧のみならずスマホアプリの利用にも影響が及ぶ事態となったことにより、情報セキュリティの観点から見れば少なくとも「可用性」が損なわれたと言うことができます。

- サーバーが攻撃を受けて停止した場合の影響は、同じサーバーでECサイトあるいはメールサーバー等も運用しているか等によっても変わってくるため、そういった事態において発生するリスクを十分に見積った上で、必要に応じCDNの採用を検討することも含め、サーバーに対する適切なセキュリティ対策の実施を計画することを推奨致します。


LAWSON
ニュースリリース NEWS RELEASE
ローソン公式ホームページおよびローソン公式アプリのサービス再開のお知らせ
2019年9月26日
9月24日（火）20時頃より、ローソン公式ホームページおよびローソン公式アプリのサービスを一時停止させていただいておりましたが、不正アタックへの防御策を講じさせていただき、9月26日（木）午前5時半より再開させていただきました。
検証の結果、現時点ではお客様への直接的な影響や個人情報の流出は確認されておりません。引き続き外部の専門機関にも依頼し徹底調査するとともに、安全性の強化のため不正アタックへの防御策を講じてまいります。
なお、グループ会社サイトおよび一部コンテンツにつきましてはサービスを停止しております。安全性の確認が取れ次第順次サービスを再開させていただきます。
お客様にご不便、ご迷惑をおかけしましたことを改めて深くお詫び申し上げます。