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。

●Linuxカーネルに脆弱性「Dirty Pipe」、アップデートの確認を

https://news.mynavi.jp/techplus/article/20220312-2291532/
https://access.redhat.com/ja/security/vulnerabilities/6802131

このニュースをザックリ言うと･･･

- 3月7日(米国時間)、米Red Hat社等より、Linuxカーネルに重大な脆弱性「CVE-2022-0847」が存在すると発表されました。

- 脆弱性は「Dirty Pipe」とも名付けられており、悪用により、本来読み取り専用のデータに対し不正に書き込みが可能となるというもので、サーバー上の攻撃者が管理者権限を奪取し、サーバー全体の乗っ取りが可能とされています。

- 脆弱性はカーネルバージョン5.8以降に影響し、2月末の時点でカーネルのセキュリティアップデート(バージョン5.16.11, 5.15.25, 5.10.102)がリリース、各種ディストリビューションにおいてもアップデートが提供されているため、適用が強く推奨されています。

AUS便りからの所感等

- 脆弱性は、例えばWebサービス等を介して直接悪用することは基本的に不可能とされていますが、ローカルにログイン可能なユーザーに悪意を持つものがいる場合や、他の脆弱性を悪用してログインに成功した攻撃者によって悪用される恐れがあることに注意が必要です。

- カーネルバージョン5.8は2020年8月にリリースされ、CentOS 8(および派生ディストリビューション)、Debian 11(Bullseye)、Ubuntu 20.04(Focal)・21.10(Impish)等、多くのディストリビューションに付属するカーネルが脆弱性の影響を受けます。

- CentOS 7、Debian 10(Buster)、Ubuntu 18.04(Bionic)のように、長期間サポートされているバージョンにおいて5.8より前のカーネルが使用され、今回の脆弱性がたまたま存在しないケースはあるものの、カーネルには他にも多数の脆弱性が随時報告され、セキュリティアップデートがリリースされているため、各種ソフトウェアを含めディストリビューションから提供されるパッケージを最新バージョンに保つように適宜アップデートを実施する管理体制を整えてください。

TECH+ Powered by マイナビニュース

Linuxカーネルに特権昇格の脆弱性、アップデートを

2022/03/09 15:16　　著者：後藤大地

Red Hatは3月7日(米国時間)、「Red Hat Customer Portal - CVE-2022-0847」において、Linuxカーネルに特権昇格につながる脆弱性が存在すると伝えた。この脆弱性は任意の読み取り専用ファイルにデータを上書きすることを可能にするものであり、この挙動を悪用することで非特権プロセスがルートプロセスにコードを注入して特権昇格が行えるようになるとされている。

脆弱性の詳細については次のページに説明がまとまっている。

- The Dirty Pipe Vulnerability - The Dirty Pipe Vulnerability documentation

Start　Software　Blog　Team　Career　©M4all

The Dirty Pipe Vulnerability

Max Kellermann <max.kellermann@ionos.com>

Abstract

This is the story of CVE-2022-0847, a vulnerability in the Linux kernel since 5.8 which allows overwriting data in arbitrary read-only files. This leads to privilege escalation because unprivileged processes can inject code into root processes.

It is similar to CVE-2016-5195 "Dirty Cow" but is easier to exploit.

●アニメーション制作会社への不正アクセスにより新作アニメの放送が延期へ

https://pc.watch.impress.co.jp/docs/news/1394959.html
https://corp.toei-anim.co.jp/ja/press/press3317734943536499054.html
https://corp.toei-anim.co.jp/ja/press/press3317734943536499055.html

このニュースをザックリ言うと・・・

- 3月7日(日本時間)、東映アニメーション株式会社より、同6日に同社システムが不正アクセスを受け、システムの一部を停止したと発表されました。

- 同11日には、これにより同社制作の一部アニメ作品の放送スケジュールに影響を及ぼすことが判明したことが発表されています。

- 既に13日以降の放送については放送済みエピソードの再放送等に差し替えられており、現時点で3月中～4月初頭まで差し替えが決定している模様です。

AUS便りからの所感

- 2月以降のロシア・ウクライナ情勢を受け、国内企業等へのサイバー攻撃の可能性について政府から注意喚起が出されており、3月初頭にはトヨタ自動車が、取引先製造会社がサイバー攻撃を受けたことにより、工場の操業を一時停止する事態となりました。

- 企業へのサイバー攻撃の成功は、不正アクセスの発生による情報流出(機密性への影響)や評判への影響のみならず、システムの稼働への影響(可用性・完全性への影響)をも及ぼす可能性があり、各種サイバー攻撃が成立する可能性および成立した場合の被害を抑制できるよう、アンチウイルスやUTMを含めた高耐性かつ速やかな復旧が可能なシステム・ネットワーク構成の検討を強く推奨致します。

Impress Watch

「プリキュア」などが再放送になったのは、東映アニメーションへの不正アクセスが原因

関根 慎一　2022年3月14日 10:32

東映アニメーション株式会社は11日、同社のネットワークに対する不正アクセスの影響で、一部アニメ作品の放映スケジュールに変更が発生したと発表した。

6日に不正アクセスが判明したことを受けて、社内のシステムを停止した影響によるもの。制作進行に支障が生じた。東映アニメーションでは不正アクセスの詳細について公表していないが、外部機関による調査を実施しており、不正アクセスされたデータに顧客の個人情報や取引先に関する情報が含まれているかどうかを確認中とのこと。

● Emotetの「進化」に対応したEmocheck 2.1.1リリース、再度の確認を

https://internet.watch.impress.co.jp/docs/news/1393399.html
https://github.com/JPCERTCC/EmoCheck/releases
https://www.jpcert.or.jp/at/2022/at220006.html

このニュースをザックリ言うと・・・

- 3月15日(日本時間)、JPCERT/CCから提供されているEmotet感染チェックツール「Emocheck」のバージョン2.1.1がリリースされています。

- JPCERT/CCでは2月10日に、昨年活動再開していたEmotetの急速な拡大について注意喚起を出していました(AUS便り2022/02/15号)が、その際に確認されたEmotetの挙動の変化に対応すべく、その後3月7日にEmocheckについても更新バージョン2.1をリリースしていました。

- 今回の2.1.1はバグを修正したものとなっており、以前に2.0等古いバージョンで実行していた場合でも今回の2.1.1を改めて実行し、チェックを行うよう推奨しています。

AUS便りからの所感

- JPCERT/CCではEmotetに関する情報のページを随時更新しており、2月17日更新の時点ではEmocheckバージョン2.0で最新のEmotetにも対応するとしていましたが、その後例外が確認されたとみられ、前述のように2.1および2.1.1をリリースしています。

- 2.1.1で修正されたバグは、管理者権限での実行時にログファイルが生成されないというもので、事前に2.1の実行でログファイルの生成が確認できた場合を除き、2.1.1での確認を怠りなく実施すべきでしょう。

- Emotetについてはこれまでもビジネス上のメールやデータのやり取りを模倣して巧みに感染しようとする手口を弄している他、今後もその挙動は刻々と変化し、UTMやアンチウイルスの検知をすり抜けて感染する可能性があり、前述のJPCERT/CC等からの情報や、Emocheckの更新について随時対応し、場合によってはデータ等のやり取りの方法を見直す等により、感染の恐れを効果的に抑止する環境を構築することが肝要です。

Impress Watch

Emotet感染確認ツール「EmoCheck」v2.1をJPCERT/CCが公開、2月に更新された挙動の変化に対応

旧バージョンで感染確認できなくても再チェックを

山田 貞幸　2022年3月8日 12:27

一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）は3月4日、マルウェア「Emotet（エモテット）」の感染有無確認ツール「EmoCheck」のv2.1を公開した。2月にアップデートされたEmotetの挙動の変化に対応し、一部の機能ロジックを改善したとしている。

[追記：3月15日 11:00]

3月14日、「EmoCheck」v2.1.1が公開された。v2.1を管理者権限で実行した際に、正しくチェックできない（プロンプトが一瞬だけ表示されて、ログファイルが作成されない）バグを修正したとしている。