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。

## ●バージョン管理システム「Git」に重大な脆弱性、2.45.1へのアップデートを…不審なレポジトリにも注意

https://forest.watch.impress.co.jp/docs/news/1591601.html
https://github.blog/2024-05-14-securing-git-addressing-5-new-vulnerabilities/
https://www.itmedia.co.jp/news/articles/2403/11/news060.html

### このニュースをザックリ言うと･･･

- 5月15日(日本時間)、バージョン管理システム「Git」の開発元より、Gitに5件の脆弱性が確認されたと発表されました。

- 最も危険度の高い脆弱性(CVE-2024-32002)はWindows・Macでも影響し、Gitレポジトリのクローン時に不正なコマンドが実行される等の恐れがあるとしています。

- 各脆弱性を修正したセキュリティアップデート2.45.1等がリリースされており、現時点でWindows版インストーラーが用意されています。

- Git開発元では、セキュリティアップデートの適用はもちろん、信頼できないソースレポジトリのクローンは行わないよう呼び掛けています。

### AUS便りからの所感等

- CVE-2024-32002は、別のレポジトリをあるレポジトリの一部として参照する「サブモジュール」機能に問題があるもので、サブモジュール側が細工を行うことにより、攻撃が可能になるとされています。

- Git関連のソフトウェアでは、1月に「GitLab」でも危険度が高いとされる脆弱性が発覚・修正されています(AUS便り 2024/01/31号参照)。

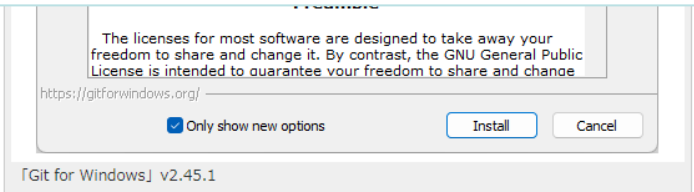
- ソースコード管理・共有サイト「Github」において、既存のリポジトリを「フォーク」した上でマルウェア等悪意のあるコードを含めたものを公開しているケースも報告されており、開発時のソースコードにマルウェアが含まれてしまい、いわゆる「サブライチェーン攻撃」を仕掛けられることがないよう、使用するレポジトリを慎重に選定する等の行動が必要です。

Impress Watch

**「Git」に深刻度「Critical」の脆弱性 ～「Git for Windows 2.45.1」などが公開**

リモートコード実行などにつながるおそれ

樽井 秀人　2024年5月15日 14:29



「Git for Windows」v2.45.1

「Git for Windows」で5月15日（日本時間）、セキュリティアップデートが実施された。現在、以下のバージョンが利用可能。

- Git for Windows v2.45.1
- Git for Windows v2.44.1
- MinGit for Windows v2.43.4
- MinGit for Windows v2.39.4

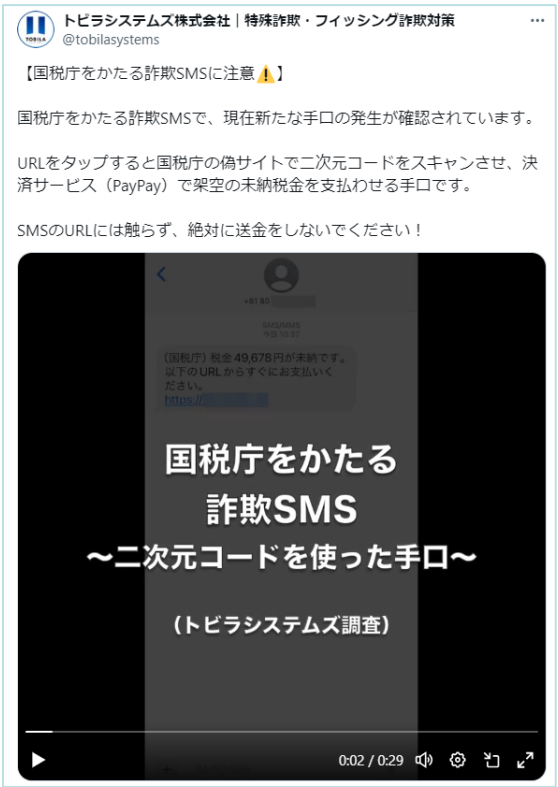
「Git」で発見された5件の脆弱性が修正されたほか、多くの不具合が修正されている。

## ●国税庁を騙るSMS→QRコードで不正送金を行わせる詐欺に注意喚起

https://twitter.com/tobilasystems/status/1790315909053284671
https://www.nta.go.jp/information/attention/attention.htm
https://paypay.ne.jp/help/c0176/

### このニュースをザックリ言うと・・・

- 5月14日(日本時間)、国内セキュリティベンダーのトビラシステムズ社より、国税庁を騙る詐欺SMSについて、同社のX(旧Twitter)アカウントで注意喚起が出されています。
- 税金が未払いであると称し、記載されたURLから偽の支払いサイトに誘導し、PayPayアプリにQRコードを読み取らせて送金を行わせる手口が動画で紹介されています。
- 同社では、SMSのURLには触らず、絶対に送金をしないよう呼び掛けるとともに、国税庁・PayPayの注意喚起ページへもリンクしています。




### AUS便りからの所感

- 国税庁は、同庁、国税局および税務署が、SMSでURLを記載した案内を送る、あるいはSMS・メールで国税の納付を求めたり差押えに関する連絡を送ることはないとしています。
- この手の不正送金詐欺はクレジットカード情報の入力を要求するケース等も既によく知られており、関係する官公庁・公的機関や、カード会社をはじめとした決済業者より、これまでに確認された様々な詐欺の事例とともに注意喚起が出ています。
- 不審なメール・SMSが届いたら、前述の注意喚起やX等ネット上で同様の事例の報告がないか、あるいは本物なのか裏をとり、常に慎重に行動することが重要です。

## ●月例のセキュリティアップデート、Microsoft・Adobeからリリース

https://forest.watch.impress.co.jp/docs/news/1591519.html
https://msrc.microsoft.com/blog/2024/05/202405-security-update/
https://forest.watch.impress.co.jp/docs/news/1591569.html

### このニュースをザックリ言うと・・・

- 5月15日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。
- Windowsの最新バージョンはWindows 10 22H2 KB5037768(ビルド 19045.4412)および11 23H2 KB5037771(ビルド 22631.3593)となります。
- MSから今回発表された脆弱性では、SharePoint Serverに関する1件が最も深刻なものとされている他、既に悪用が確認されている、いわゆる「ゼロデイ」のものがWindowsで2件、Visual Studioで1件報告されています。
- 同日にはAdobe社からもAcrobat・Acrobat Reader・Illustrator等に対するセキュリティアップデートがリリースされています。

### AUS便りからの所感

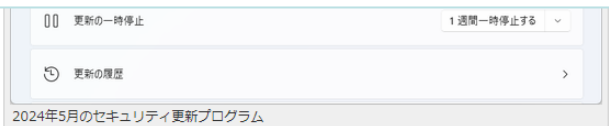
- JPCERT/CCやIPAからも月例アップデートに合わせて注意喚起が出されており、特にWindowsのゼロデイ脆弱性やAcrobat・Acrobat Readerに対する対策を速やかに行うよう呼び掛けられています。
- またEdgeブラウザーについても、月例以外のタイミングでのアップデートながら、最新バージョン124.0.2478.105がリリースされており、バージョン情報の確認および手動での更新実行を推奨致します(Chromeについてもここ最近頻繁にアップデートがあり、同様に現時点での最新バージョン124.0.6367.207やそれ以降への更新を確認しましょう)。
- 今後発生し得る新たな攻撃に備え、OSや機器のファームウェアあるいは各種アプリケーションに至るまで確実にアップデートを適用すること、それまでに発生する攻撃に対しアンチウイルス・UTM等による防御策をとることが肝要です。

Impress Watch

**2024年5月の「Windows Update」がリリース、緊急の脆弱性やゼロデイ脆弱性も**

CVE番号ベースで59件の問題へ新たに対処

樽井 秀人　2024年5月15日 10:41




米Microsoftは5月14日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで59件の脆弱性が新たに対処されている。