サイバー攻撃対策通信 （令和7年第9号）	令和７年8月26日 福岡県警察

サポートが終了しているパッチ未適用のCisco製通信機器が標的に

令和７年８月20日、FBI及びCiscoは、ロシアによる既知の脆弱性（CVE-2018-0171、CVSS:9.8)を悪用する攻撃について以下のとおり警告しました。
昨今は、Cisco製通信機器以外でも、既知の脆弱性が悪用されるケースが増えているため、今一度組織内の通信機器を確認することを推奨いたします。

CVE-2018-0171は、Cisco IOS/IOS XEソフトウェアのスマートインストール機能（SMI）機能で使用するポート4786の影響をうける通信機器に、入力検証の不備を突かれて細工されたSMIメッセージを送付され、サービス拒否状態や任意のコードを実行されるもの。

FBI

- **過去１年間にわたり、重要インフラの米国企業に関連する何千台ものインフラ関連の通信機器から構成ファイルを収集した。**
- **収集した構成ファイルを改変し、不正アクセスを永久的に確保した。**

Cisco

- 主な標的は、北米、**アジア**、ヨーロッパの通信、高等教育、製造業である。
- ロシアだけに留まらず、他の国家支援を受けた攻撃者も本脆弱性を悪用した攻撃を実行している可能性がある。

対応策

- ソフトウェアアップデート
- 使用不要の場合はSmart Installの無効化を推奨

暫定的な回避策は存在しない

IoC情報

IPアドレス	既知のアクティビティ	IPアドレス	既知のアクティビティ
185.141.24.222	2023年3月23日	185141.24.28	2024年10月1日～2025年7月3日
185.82.200.181	2024年10月1日～	185.82.202.34	2025年1月15日～同年2月28日

参考URL
① https://blog.talosintelligence.com/static-tundra/　② https://www.ic3.gov/PSA/2025/PSA250820

福岡県警察サイバー攻撃対策隊（公安第一課第七係）電話番号：092-641-4141(5986)