【参考】
ランサムウェアを用いる攻撃者グループによる悪用が報告されているソフトウェアや機器等の脆弱性について（令和３年６月28日付厚生労働省事務連絡より抜粋）

チェックポイント

- インターネット等外部ネットワークからアクセス可能な機器については、外部ネットワーク公開の必要性を十分検討したうえで、セキュリティパッチを迅速に適用する、外部からの管理機能、不要なポート(137(TCP/UDP)、138(UDP)、139(TCP)、445(TCP/UDP)、3389(TCP/UDP)など)やプロトコルを外部に開放しない等の対応策等、IT資産管理を改めて確認する。特に、通信プロトコル「SMB」や「RDP」については、これまでも必要最小限のポートの開放やSMBv1の無効化等を呼びかけているところ、ファイアウォールを含む各機器の設定を改めて確認する。
- ソフトウエアや機器等の脆弱性については、ランサムウエアを用いる攻撃者グループによる悪用が報告されているものを含む以下の脆弱性に十分留意する。
  - Fortinet製Virtual Private Network(VPN)装置の脆弱性(CVE-2018-13379)[2]
  - Ivanti製VPN装置「Pulse Connect Secure」の脆弱性(CVE-2021-22893、CVE-2020-8260、CVE-2020-8243、CVE-2019-11510)[3]
  - Citrix製「Citrix Application Delivery Controller」「Citrix Gateway」「Citrix SD-WAN WANOP」の脆弱性(CVE-2019-19781)[4]
  - Microsoft Exchange Serverの脆弱性(CVE-2021-26855等)[5]
  - SonicWall Secure Mobile Access (SMA) 100シリーズの脆弱性(CVE-2021-20016)[6]
  - QNAP Systems製NAS(Network Attached Storage)製品「QNAP」に関する脆弱性(CVE-2021-28799、CVE-2020-36195、CVE-2020-2509等)[7]
  - Windowsのドメインコントローラーの脆弱性(CVE-2020-1472等)[8]
- テレワーク等に関連し、職場から持ち出したPCについて、休暇中に長期間、十分な管理下になかったPCを職場で再び利用する際は、パッチの適用やウイルススキャンの実施など必要に応じて実施する。
- 最近では、マルウエア「Emotet」に代わり、マルウエア「IcedID」に感染させる不正なメール等も確認されていることから、ウイルス対策ソフトの導入及び最新化、定期スキャンの実施、メール環境に対するセキュリティ対策等、通常のマルウエア対策も実施する。

---

[2] *NISC「Fortinet製VPNの脆弱性(CVE-2018-13379)に関する重要インフラ事業者等についての注意喚起の発出について(2020/12/3)」、https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf (2021/4/30閲覧)*

[3] *Ivanti「Pulse Connect Secure Security Update(2021/4/20)」、https://blog.pulsesecure.net/pulse-connect-secure-security-update/ (2021/4/30閲覧)*

[4] *Citrix「CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance(2020/10/23)」、https://support.citrix.com/article/CTX267027 (2021/4/30閲覧)*

[5] *Microsoft「On-Premises Exchange Server Vulnerabilities Resource Center(2021/3/25)」、https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/ (2021/4/30閲覧)*

[6] *SonicWall「CONFIRMED ZERO-DAY VULNERABILITY IN THE SONICWALL SMA100 BUILD VERSION 10.X(2021/4/30)」、https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001 (2021/4/30閲覧)*

[7] *QNAP Systems「Response to Qlocker Ransomware Attacks: Take Actions to Secure QNAP NAS(2021/4/22)、https://www.qnap.com/en/security-news/2021/response-to-qlocker-ransomware-attacks-take-actions-to-secure-qnap-nas (2021/4/30閲覧)*

[8] *Microsoft「CVE-2020-1472 Netlogon の特権の昇格の脆弱性(2021/2/9)」、https://msrc.microsoft.com/update-guide/ja-jp/vulnerability/CVE-2020-1472 (2021/4/30閲覧)*