内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

2021 年 5 月 7 日

内閣官房内閣サイバーセキュリティセンター

大型連休明けに確認が必要な情報について

2021 年 5 月 7 日、内閣サイバーセキュリティセンターは、重要インフラ事業者等に向けて、大型連休明けに確認が必要な情報について注意喚起を行いました。

本件は、日本国内においても、ランサムウエアの感染により、データが暗号化されたり、業務情報や個人情報が窃取されたりする事例が相次いで確認されていること等を踏まえ、大型連休明けに確認が必要となる情報について、重要インフラ事業者等の十全なサイバーセキュリティ確保のための注意喚起ですが、広く一般にも活用していただけるよう公開するものです。

資料：大型連休明けに確認が必要な情報について(注意喚起)

本件に対する問い合わせ先
内閣サイバーセキュリティセンター(NISC)
電話：03-5253-2111(代表)
重要インフラ第 2 グループ

2021 年 5 月 7 日

内閣サイバーセキュリティセンター
重要インフラグループ

大型連休明けに確認が必要な情報について(注意喚起)

大型連休明けに確認が必要な情報について、情報提供します。これらの情報を確認し、重要インフラ事業者等の十全なサイバーセキュリティ確保に努めてください。

1. 新種のランサムウエア「FiveHands」に関する解析レポートの発行について

米国 CISA は、新種のランサムウエア「FiveHands」に関する解析レポートを公開しました。CISA によると、VPN 装置の脆弱性を悪用し、本ランサムウエアに感染させる事例が確認されているとのことです。ランサムウエアに関して、当センターから「ランサムウエアによるサイバー攻撃に関する注意喚起について」(2021 年 4 月 30 日)を発出していたところ、参考 URL を参照し、攻撃の手口や特徴を確認することを推奨します。

参考 URL
- CISA Releases Analysis Reports on New FiveHands Ransomware(CISA)
  https://us-cert.cisa.gov/ncas/current-activity/2021/05/06/cisa-releases-analysis-reports-new-fivehands-ransomware
- Analysis Report(AR21-126A) FiveHands Ransomware(CISA)
  https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a
- Malware Analysis Report(AR21-126B) MAR-10324784-1.v1: FiveHands Ransomware (CISA)
  https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126b
- UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat (FireEye)
  https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html
- ランサムウエアによるサイバー攻撃に関する注意喚起について(NISC)
  https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf

2. Ivanti 製 VPN 製品「Pulse Connect Secure」のセキュリティパッチの公開について

(1) 対象製品

- Pulse Connect Secure 9.1Rx
- Pulse Connect Secure 9.0Rx

Ivanti 製 VPN 製品「Pulse Connect Secure」には、悪用された場合、当該製品を経由して組織内部に侵入され、機密情報が窃取等される恐れがある脆弱性[CVE-2021-22893]が存在しています。これまで、本脆弱性に対するセキュリティパッチは公開されておらず、「Ivanti 製 VPN 製品「Pulse Connect Secure」、オラクル製ソ

フトウエア及びグーグル製「Chrome」の深刻な脆弱性について(注意喚起)」(2021 年 4 月 21 日)において、回避策の実施等に関して注意喚起していたところ、2021 年 5 月 3 日、本脆弱性のセキュリティパッチが公開されました。なお、本セキュリティパッチには、この脆弱性[CVE-2021-22893]の他、別の脆弱性[CVE-2021-22894、CVE-2021-22899、CVE-2021-22900]の修正も含まれています。

(2) 対応

対象製品を最新のバージョンに更新。

更新方法等については、参考 URL 参照。

参考 URL
- Pulse Connect Secure Patch Availability - SA44784(Ivanti)
  https://blog.pulsesecure.net/pulse-connect-secure-patch-availability-sa44784
- SA44784 - 2021-04: Out-of-Cycle Advisory: Multiple Vulnerabilities Resolved in Pulse Connect Secure 9.1R11.4(Ivanti)
  https://kb.pulsesecure.net/articles/Pulse_Secure_Article/SA44784/
- Ivanti Releases Pulse Secure Security Update(CISA)
  https://us-cert.cisa.gov/ncas/current-activity/2021/05/03/ivanti-releases-pulse-secure-security-update
- 更新：Pulse Connect Secure の脆弱性対策について(CVE-2021-22893)(IPA)
  https://www.ipa.go.jp/security/ciadr/vul/alert20210421.html
- Pulse Connect Secure の脆弱性 (CVE-2021-22893) に関する注意喚起(JPCERT/CC)
  https://www.jpcert.or.jp/at/2021/at210019.html

3. VMware 製ソフトウエア「VMware vRealize Business for Cloud」について

(1) 対象ソフトウエア

・VMware vRealize Business for Cloud 7.6 より前のバージョン

上記ソフトウエアには、VMware が深刻度「Critical」(4 段階中、最高)に分類するリモートコード実行が可能な脆弱性(CVE-2021-21984)に対する修正が含まれており、詳細については、参考 URL を参照してください。

(2) 対応

対象ソフトウエアを最新のバージョンに更新。

更新方法等については、参考 URL 参照。

参考 URL
- VMSA-2021-0007(VMware)
  https://www.vmware.com/security/advisories/VMSA-2021-0007.html
- vRealize Business for Cloud 7.6 Security Build for VMSA-2021-0007(83475)(VMware)
  https://kb.vmware.com/s/article/83475
- Security Response Policy(VMware)
  https://www.vmware.com/support/policies/security_response.html

4. Cisco Systems 製品について

(1) 対象製品

・Cisco SD-WAN vManage、Cisco HyperFlex HX 等を含む複数の Cisco Systems 製品

上記製品には、認証されていない第三者がリモートでコードを実行可能な脆弱性等に対する修正が含まれており、詳細については、参考 URL を参照してください。

(2) 対応

対象製品を最新のバージョンに更新。

更新方法等については、参考 URL 参照。

参考 URL

・Cisco SD-WAN vManage Software Vulnerabilities(Cisco Systems)
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-4TbynnhZ

・Cisco HyperFlex HX Command Injection Vulnerabilities(Cisco Systems)
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR

・Cisco Releases Security Updates for Multiple Products(CISA)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/06/cisco-releases-security-updates-multiple-products