ＮＩＳＣ重要インフラニュースレター第２９３号

中国地域サイバーセキュリティ連絡会の皆様へ

中国地域サイバーセキュリティ連絡会　事務局の木坂です。

NISCより、重要インフラニュースレター第２９３号（９／１４）が
下記のとおり発行されましたので、お送りいたします。
（必要に応じて幅広く展開していただいて結構です）

既にご購読の方で、配信不要の場合は事務局までお知らせください。

■━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━□
┃　　　◆◆　NISC重要インフラニュースレター　◆◆
┃　　　　　　（２０２１年9月１４日発行 第２９３号）
┃　　　　　　　　　　　　　　　　発行：NISC重要インフラグループ
□━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━■

┼─◎ はじめに ──────────────┼
　重要インフラニュースレターは、重要インフラの関係者を中心に情報セキュリティに関する情報を幅広く紹介するものです。
　情報システム部門の担当者から管理職や経営層の方まで必要に応じて幅広く共有いただければ幸いです。
┼──────────────────────────────┼

┌◆　第２９３号の目次　◆──────────────────┐

├──────────────────────────────┤
○今号は、８月２４日～９月１３日頃の記事を集めて編集しています。
└──────────────────────────────┘

１．チェックが必要な情報

（１）Microsoft 製品に関する脆弱性

・Microsoft MSHTML の脆弱性(CVE-2021-40444)に関する注意喚起(IPA、JPCERT/CC、米国 DHS)(09/07、09/08、09/09)

https://www.jpcert.or.jp/at/2021/at210038.html

https://www.ipa.go.jp/security/ciadr/vul/20210908-ms.html

https://us-cert.cisa.gov/ncas/current-activity/2021/09/07/microsoft-releases-mitigations-and-workarounds-cve-2021-40444

（２）Mozilla 製品に関する脆弱性

・Mozilla が Firefox、Firefox ESR 及び Thunderbird のセキュリィティアップデートをリリース(米国 DHS)(09/08)

https://us-cert.cisa.gov/ncas/current-activity/2021/09/08/mozilla-releases-security-updates-firefox-firefox-esr-and

（３）Google 製品(Chrome)に関する脆弱性

・Google が Chrome のセキュリティアップデートをリリース(米国 DHS、Google)(09/01、09/13)

https://us-cert.cisa.gov/ncas/current-activity/2021/09/01/google-releases-security-updates-chrome

https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html

（４）VMware 製品に関する脆弱性

・VMware が複数の製品のセキュリティアップデートをリリース?(米国 DHS)(08/25)

https://us-cert.cisa.gov/ncas/current-activity/2021/08/25/vmware-releases-security-updates-multiple-products

（５）その他

・Ghostscript の任意のコマンド実行が可能な脆弱性(CVE-2021-3781)に関する注意喚起(JPCERT/CC)(09/13)

https://www.jpcert.or.jp/at/2021/at210039.html

・OpenSSL の複数の脆弱性(JPCERT/CC、JVN)(08/25)
https://www.jpcert.or.jp/at/2021/at210036.html
https://jvn.jp/vu/JVNVU99612123/

・複数のソニー製品のインストーラにおける DLL 読み込みに関する脆弱性(JVN)(08/24)
https://jvn.jp/jp/JVN80288258/
※CVSSv3 では基本値「7.8」となっています。

・Delta Electronics 製 TPEditor にヒープベースのバッファオーバーフローの脆弱性(JVN)(08/25)
https://jvn.jp/vu/JVNVU97299655/
※CVSSv3 では基本値「7.8」となっています。

・複数の Delta Electronics 製品に複数の脆弱性(JVN)(08/27)
https://jvn.jp/vu/JVNVU99414749/
※CVSSv3 では基本値「9.8」となっています。

・Delta Electronics 製 DOPSoft 2 に複数の脆弱性(JVN)(09/10)
https://jvn.jp/vu/JVNVU95804712/
※CVSSv3 では基本値「7.8」となっています。

・複数の Hitachi ABB Power Grids 製品に複数の脆弱性(JVN)(08/25)
https://jvn.jp/vu/JVNVU93649726/index.html
※CVSSv3 では基本値「7.7」となっています。

・Hitachi ABB Power Grids 製 System Data Manager における重要な情報の平文保存の脆弱性(JVN)(09/08)
https://jvn.jp/vu/JVNVU94275152/

・Movable Type における複数のクロスサイトスクリプティングの脆弱性(JVN)(08/25)
https://jvn.jp/jp/JVN97545738/

・Controlled Electronic Management Systems 社製 CEM Systems AC2000 における不適切な認可処理の脆弱性(JVN)(08/27)
https://jvn.jp/vu/JVNVU92147191/

・Annke 製 Network Video Recorder におけるスタックベースのバッファオーバーフローの脆弱性(JVN)(08/27)
https://jvn.jp/vu/JVNVU96392481/
※CVSSv3 では基本値「9.4」となっています。

・baserCMS におけるクロスサイトスクリプティングの脆弱性(JVN)(08/27)
https://jvn.jp/jp/JVN14134801/

・Sensormatic Electronics 製 KT-1 にメンテナンスされていないサードパーティ製品を使用している問題(JVN)(09/01)
https://jvn.jp/vu/JVNVU96796123/

・Sensormatic Electronics 製 Illustra に境界条件の判定に関する脆弱性(JVN)(09/03)
https://jvn.jp/vu/JVNVU96372273/
※CVSSv3 では基本値「7.8」となっています。

・トレンドマイクロ製ウイルスバスター クラウドにおけるディレクトリジャンクションの取り扱い不備の脆弱性(JVN)(09/02)
https://jvn.jp/vu/JVNVU94699053/

・ジェイテクト製 TOYOPUC シリーズにおける制限またはスロットリング無しのリソースの割り当ての脆弱性(JVN)(09/02)
https://jvn.jp/vu/JVNVU95792804/

・Advantech 製 WebAccess におけるスタックベースのバッファオーバーフローの脆弱性(JVN)(09/06)
https://jvn.jp/vu/JVNVU92879401/

・RevoWorks Browser における複数の脆弱性(JVN)(09/10)
https://jvn.jp/jp/JVN81658818/
※CVSSv3 では基本値「8.6」となっています。

・AVEVA 製 PCS Portal における DLL 読み込みに関する脆弱性(JVN)(09/10)
https://jvn.jp/vu/JVNVU98046090/
※CVSSv3 では基本値「7.3」となっています。

・Mitsubishi Electric Europe B.V.製 smartRTU および INEA 製 ME-RTU における複数の脆弱性(JVN)(09/13)
https://jvn.jp/vu/JVNVU93054759/
※CVSSv3 では基本値「9.8」となっています。

・EC-CUBE 用プラグイン「一覧画面(受注管理)項目変更プラグイン」におけるクロスサイトスクリプティングの脆弱性(JVN)(09/13)
https://jvn.jp/jp/JVN46313661/

２．政府機関の動き

● 警察庁
・令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について(09/09)

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf

３．関係機関の動き

（１）ＩＰＡ
・安心相談窓口だより「URL リンクへのアクセスに注意！」(08/31)
https://www.ipa.go.jp/security/anshin/mgdayori20210831.html

（２）ＪＰＣＥＲＴ コーディネーションセンター
・EthicsfIRST インシデント対応およびセキュリティチームのための倫理規範(日本語版)(09/07)
https://www.jpcert.or.jp/research/FIRST-EthicsfIRST.html

・Weekly Report 2021-09-01 号(09/01)
https://www.jpcert.or.jp/wr/2021/wr213401.html

・Weekly Report 2021-09-08 号(09/08)
https://www.jpcert.or.jp/wr/2021/wr213501.html

４．海外の動き

（１）米国 DHS

・FBI と CISA が休日と週末のランサムウェア認識に関するアドバイザリをリリース(08/31)
https://us-cert.cisa.gov/ncas/current-activity/2021/08/31/fbi-cisa-advisory-ransomware-awareness-holidays-and-weekends
https://us-cert.cisa.gov/ncas/alerts/aa21-243a

・CISA がパルスセキュア関連のマルウェア分析レポート(5 件)をリリース(08/24)
https://us-cert.cisa.gov/ncas/current-activity/2021/08/24/cisa-releases-five-pulse-secure-related-mars

・マルウェア分析レポート(AR21-236A-AR21-236E)(08/24)
MAR-10336935-2.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-236a
MAR-10333243-3.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-236b
MAR-10338401-2.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-236c
MAR-10334057-3.v1 パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-236d
MAR-10339606-1.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-236e

・F5 が BIG-IP 及び BIG-IQ の複数の脆弱性に関するセキュリティアドバイザリーをリリース(2021 年 8 月)(08/25)
https://us-cert.cisa.gov/ncas/current-activity/2021/08/25/f5-releases-august-

2021-security-advisory

・FBI がサイバー犯罪組織 OnePercentGroup によるランサムウェア攻撃に関連する侵入の痕跡(IOC)をリリース(08/25)
https://us-cert.cisa.gov/ncas/current-activity/2021/08/25/fbi-releases-indicators-compromise-associated-onepercent-group

・Cisco が複数の製品のセキュリティアップデートをリリース(08/26)
https://us-cert.cisa.gov/ncas/current-activity/2021/08/26/cisco-releases-security-updates-multiple-products

・Cisco が CiscoEnterpriseNFVIS のセキュリティアップデートをリリース(09/02)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/02/cisco-releases-security-updates-cisco-enterprise-nfvis

・Cisco が複数製品のセキュリティアップデートをリリース(09/09)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/09/cisco-releases-security-updates-multiple-products

・産業用制御システム合同作業部会(ICSJWG)2021 秋 Virtual Meeting(08/27)
https://us-cert.cisa.gov/ncas/current-activity/2021/08/27/icsjwg-2021-fall-virtual-meeting

・FBI がランサムウェア Hive に関連する侵入の痕跡(IOC)をリリース(08/27)
https://us-cert.cisa.gov/ncas/current-activity/2021/08/27/fbi-releases-indicators-compromise-associated-hive-ransomware

・Microsoft が Azure Cosmos DB の構成ミスの脆弱性に関するガイダンスをリリース(08/27)
https://us-cert.cisa.gov/ncas/current-activity/2021/08/27/microsoft-azure-cosmos-db-guidance

・CISA はバッドプラクティスリストに単一要素認証の使用を追加(08/30)
https://us-cert.cisa.gov/ncas/current-activity/2021/08/30/cisa-adds-single-factor-authentication-list-bad-practices

・Atlassian がコンフルエンスサーバーとデータセンターのセキュリティアップデートをリリース(09/03)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/03/atlassian-releases-security-updates-confluence-server-and-data

・CISA がマネージドサービスプロバイダー(MSP)の顧客のリスクに関する考慮事項をリリース(09/03)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/03/cisa-insights-risk-considerations-managed-service-provider

・Citrix が Hypervisor のセキュリティアップデートをリリース(09/09)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/09/citrix-releases-security-updates-hypervisor

・WordPress がセキュリティアップデートをリリース(09/10)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/10/wordpress-releases-security-update

・Apple が CVE-2021-30858 及び CVE-2021-30860 に対応するセキュリティアップデートをリリース(09/13)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/13/apple-releases-security-updates-address-cve-2021-30858-and-cve

・2021 年 8 月 23 日の週の脆弱性概報(08/30)
https://us-cert.cisa.gov/ncas/bulletins/sb21-242

・2021 年 8 月 30 日の週の脆弱性概報(09/06)
https://us-cert.cisa.gov/ncas/bulletins/sb21-249

・2021 年 9 月 6 日の週の脆弱性概報(09/13)
https://us-cert.cisa.gov/ncas/bulletins/sb21-256

・Bluetooth コア及びメッシュ仕様をサポートするデバイスに偽装攻撃及び AuthValue 開示に対する脆弱性(更新)(09/01)

https://kb.cert.org/vuls/id/799380

・Arcadyan ベースのルーターとモデムのパストラバーサルの脆弱性(更新)(09/06)
https://kb.cert.org/vuls/id/914124

・Advantech の WebAccess/SCADA に相対パストラバーサル等の脆弱性(更新)(08/24)
https://us-cert.cisa.gov/ics/advisories/icsa-21-168-03
※CVSSv3 では基本値「7.3」となっています。

・Philips の患者監視デバイスに他の領域へのリソースの漏洩等の脆弱性(更新)(08/31)
https://us-cert.cisa.gov/ics/advisories/icsma-20-254-01

・三菱電機のシーケンサ MELSEC iQ-R series に保護が不十分なクレデンシャルに関する脆弱性(09/07)
https://us-cert.cisa.gov/ics/advisories/icsa-21-250-01
※CVSSv3 では基本値「7.4」となっています。

・三菱電機の複数製品に脆弱性(更新)(09/09)
https://us-cert.cisa.gov/ics/advisories/icsa-20-245-01
※CVSSv3 では基本値「7.3」となっています。

（2）その他
・NETGEAR 製スマートスイッチに関する複数の脆弱性(NETGEAR)(09/03)
https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145

5．読者へのお願い

ニュースレターについてのご意見、ご感想、掲載を希望する記事等ございましたら以下の連絡先にご連絡下さい。
mailto:nisc-infra-letter@cyber.go.jp

６．次回予告

次回は、２０２１年９月２８日配信の予定です。
※本ニュースレターは、原則として、毎月第２・第４火曜日頃に発行しますが、都合により変則的な配信日となることがあります。

◎官民で連携した重要インフラ防護に係る取組をご紹介しています。
https://www.nisc.go.jp/active/infra/index.html

◎NISC や関係機関が作成した情報セキュリティに係る意識啓発動画を掲載しています。
https://www.youtube.com/user/NISCchannel/videos

◎本ニュースレターは、主にセプターや重要インフラ事業者等に対して、情報セキュリティに関する取組等を幅広く紹介することを目的としています。このため、掲載内容の利活用の方法や本ニュースレターの転送等について、特に制限はしておりませんが、利活用や転送等に際しては、リンク先の情報を参照の上、ご自身の責任でお願いいたします。
また、掲載情報が一部重複する場合もございますが、ご容赦願います。