ＮＩＳＣ重要インフラニュースレター第２８９号

中国地域サイバーセキュリティ連絡会へ入会頂いた皆様へ

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２８９号（7/13）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７月１３日発行 第２８９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２８９号の目次　◆──────────────┐

├────────────────────────────────┤

○今号は、６月２２日～７月１２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 Windows 製品の Windows Print Spooler の脆弱性について(IPA、JPCERT/CC、JVN、米国 DHS、米国 CERT/CC)(07/01、07/05、07/06、07/08)
https://www.ipa.go.jp/security/ciadr/vul/20210705-ms.html
https://www.jpcert.or.jp/at/2021/at210029.html
https://jvn.jp/vu/JVNVU96262037/
https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability
https://us-cert.cisa.gov/ncas/current-activity/2021/07/06/microsoft-releases-out-band-security-updates-printnightmare
https://kb.cert.org/vuls/id/383432
※CVSSv3 では基本値「8.8」となっています。

（2）その他

・JPCERT/CC Eyes「EC サイトのクロスサイトスクリプティング脆弱性を悪用した攻撃」(JPCERT/CC)(07/06)
https://blogs.jpcert.or.jp/ja/2021/07/water_pamola.html

・複数の Exacq Technologies 製品にクロスサイトスクリプティングの脆弱性(JVN)(06/30)
https://jvn.jp/vu/JVNVU94425254/

・パナソニック製 FPWIN Pro に XML 外部エンティティ参照の不適切な制限の脆弱性(JVN)(06/30)
https://jvn.jp/vu/JVNVU95869186/

・AVEVA 製 AVEVA System Platform における複数の脆弱性(JVN)(06/30)
https://jvn.jp/vu/JVNVU90207343/
※CVSSv3 では基本値「8.0」となっています。

・Claroty 製 Secure Remote Access Site に認証回避の脆弱性(JVN)(06/30)
https://jvn.jp/vu/JVNVU91235385/

・EC-CUBE におけるアクセス制限不備の脆弱性(JVN)(07/01)
https://jvn.jp/jp/JVN57942445/
※CVSSv3 では基本値「7.5」となっています。

・三菱電機製空調管理システムにおける XML 外部実体参照(XXE)の不適切な制限に関する脆弱性(JVN)(07/01)
https://jvn.jp/vu/JVNVU93086468/
※CVSSv3 では基本値「9.3」となっています。

・三菱電機製空調管理システムの WEB 機能における認証アルゴリズムの不適切な実装に関する脆弱性(JVN)(07/01)
https://jvn.jp/vu/JVNVU96046575/
※CVSSv3 では基本値「7.1」となっています。

・Johnson Controls 製 Facility Explorer に不適切な権限管理の脆弱性(JVN)(07/02)
https://jvn.jp/vu/JVNVU91813797/
※CVSSv3 では基本値「8.8」となっています。

・Sensormatic Electronics 製 C-CURE 9000 に不適切な入力確認の脆弱性(JVN)(07/02)
https://jvn.jp/vu/JVNVU95301283/
※CVSSv3 では基本値「8.8」となっています。

・Bachmann Electronic 製 M1 System Processor Modules における強度が不十分なパスワードハッシュの使用の脆弱性(JVN)(07/02)
https://jvn.jp/vu/JVNVU98660055/
※CVSSv3 では基本値「7.2」となっています。

・トレンドマイクロ製パスワードマネージャーにおける複数の脆弱性(JVN)(07/05)
https://jvn.jp/vu/JVNVU93149000/

・株式会社 A-Stage 製 SCT-40CM01SR および AT-40CM01SR における認証不備の

脆弱性(JVN)(07/05)
https://jvn.jp/jp/JVN21636825/

・WordPress 用プラグイン WordPress Email Template Designer - WP HTML Mail におけるクロスサイトリクエストフォージェリの脆弱性(JVN)(07/06)
https://jvn.jp/jp/JVN42880365/

・WordPress 用プラグイン WPCS - WordPress Currency Switcher におけるクロスサイトリクエストフォージェリの脆弱性(JVN)(07/06)
https://jvn.jp/jp/JVN91372527/

・WordPress 用プラグイン Software License Manager におけるクロスサイトリクエストフォージェリの脆弱性(JVN)(07/08)
https://jvn.jp/jp/JVN89054582/

・WordPress 用プラグイン WordPress Meta Data Filter & Taxonomies Filter におけるクロスサイトリクエストフォージェリの脆弱性(JVN)(07/08)
https://jvn.jp/jp/JVN48413554/

・エレコム製ルータにおける認証不備および OS コマンドインジェクションの脆弱性(JVN)(07/06)
https://jvn.jp/vu/JVNVU94260088/

・Philips 製 Vue PACS 製品における複数の脆弱性(JVN)(07/07)
https://jvn.jp/vu/JVNVU96012689/
※CVSSv3 では基本値「9.8」となっています。

・Moxa 製 NPort IAW5000A-I/O Series Wireless Device Server に複数の脆弱性(JVN)(07/07)
https://jvn.jp/vu/JVNVU98641659/
※CVSSv3 では基本値「9.8」となっています。

・Android アプリ「ジーユー」におけるアクセス制限不備の脆弱性(JVN)(07/07)
https://jvn.jp/jp/JVN25850723/

・Rockwell Automation 製 MicroLogix 1100 における不適切な入力確認の脆弱性(JVN)(07/09)
https://jvn.jp/vu/JVNVU93901835/
※CVSSv3 では基本値「8.6」となっています。

・MDT Software 製 MDT AutoSave に複数の脆弱性(JVN)(07/09)
https://jvn.jp/vu/JVNVU95888908/
※CVSSv3 では基本値「10.0」となっています。

・Everything における HTTP ヘッダインジェクションの脆弱性(JVN)(07/09)
https://jvn.jp/jp/JVN68971465/

２．政府機関の動き

（１）ＮＩＳＣ

・サイバーセキュリティ戦略本部第 30 回会合を開催(07/07)
https://www.nisc.go.jp/conference/cs/index.html#cs30

・「次期サイバーセキュリティ戦略(案)」等に関する意見の募集について(07/12)
https://www.nisc.go.jp/active/kihon/cyber-security-senryaku_2021.html

（２）金融庁

・「金融機関の IT ガバナンス等に関する調査結果レポート」及び「金融機関のシステム障害に関する分析レポート」の公表について(06/30)
https://www.fsa.go.jp/news/r2/20210630/20210630.html

（３）総務省

・ 「スマートシティセキュリティガイドライン（第 2.0 版）」（案）に対する意見募集の結果及び「スマートシティセキュリティガイドライン（第 2.0 版）」の公表(06/30)
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00115.html

３．関係機関の動き

（１）ＩＰＡ

・安心相談窓口だより「安易に運転免許証など本人確認書類の写真を送信しないで！」(06/23)

https://www.ipa.go.jp/security/anshin/mgdayori20210623.html

・「サイバーレスキュー隊（J-CRAT）活動状況 2020 年度下半期」を公開しました(06/25)

https://www.ipa.go.jp/security/J-CRAT/index.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2021-06-23 号(06/23)

https://www.jpcert.or.jp/wr/2021/wr212401.html

・Weekly Report 2021-06-30 号(06/30)

https://www.jpcert.or.jp/wr/2021/wr212501.html

・Weekly Report 2021-07-07 号(07/07)

https://www.jpcert.or.jp/wr/2021/wr212601.html

・CyberNewsFlash「2021 年 4 月から 6 月を振り返って」(07/08)

https://www.jpcert.or.jp/newsflash/2021070801.html

４．海外の動き

（１）米国 DHS

・CISA がマルウェア分析レポートを公開し、DarkSide ランサムウエアに関するアラートを更新(07/07、07/08)

https://us-cert.cisa.gov/ncas/current-activity/2021/07/07/cisa-publishes-malware-analysis-report-and-updates-alert-darkside

https://us-cert.cisa.gov/ncas/alerts/aa21-131a

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-148a

・VMware はセキュリティアップデートをリリース(06/23)

https://us-cert.cisa.gov/ncas/current-activity/2021/06/23/vmware-releases-

security-updates

・Citrix は Hypervisor のセキュリティアップデートをリリース(06/25)
https://us-cert.cisa.gov/ncas/current-activity/2021/06/25/citrix-releases-security-updates-hypervisor

・CISA はサイバーリスクを高める悪い慣行のカタログ作成を開始(06/29)
https://us-cert.cisa.gov/ncas/current-activity/2021/06/29/cisa-begins-cataloging-bad-practices-increase-cyber-risk

・CISA のサイバーセキュリティ評価ツール(CSET)はランサムウエアの脅威に照準を設定(06/30)
https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat

・ロシアの GRU によるブルートフォースキャンペーンに関する NSA-CISA-NCSC-FBI 共同サイバーセキュリティアドバイザリー(07/01)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/01/nsa-cisa-ncsc-fbi-joint-cybersecurity-advisory-russian-gru-brute

・Kaseya VSA のサプライチェーンランサムウエア攻撃(07/02)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/02/kaseya-vsa-supply-chain-ransomware-attack

・Kaseya VSA のサプライ チェーン ランサムウエア攻撃の影響を受ける MSP とその顧客に対する CISA-FBI ガイダンス(07/04)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

・Kaseya は VSA オンプレミスソフトウェアの脆弱性に対するセキュリティアップデートを提供(07/12)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/12/kaseya-provides-security-updates-vsa-premises-software

・Cisco は複数製品のセキュリティアップデートをリリース(07/08)

https://us-cert.cisa.gov/ncas/current-activity/2021/07/08/cisco-releases-security-updates-multiple-products

・CISA が FY20 のリスクと脆弱性の評価の分析をリリース(07/08)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/08/cisa-releases-analysis-fy20-risk-and-vulnerability-assessments

・ForgeRock アクセス管理の重大な脆弱性(07/12)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/12/critical-forgerock-access-management-vulnerability

・2021 年 6 月 21 日の週の脆弱性概報(06/28)
https://us-cert.cisa.gov/ncas/bulletins/sb21-179

・2021 年 6 月 28 日の週の脆弱性概報(07/05)
https://us-cert.cisa.gov/ncas/bulletins/sb21-186

・2021 年 7 月 5 日の週の脆弱性概報(07/12)
https://us-cert.cisa.gov/ncas/bulletins/sb21-193

・FATEK の WinProladder には範囲外読み取りの脆弱性(06/24)
https://us-cert.cisa.gov/ics/advisories/icsa-21-175-01
※CVSSv3 では基本値「7.8」となっています。

・Philips の相互運用性ソリューション XDS には機密情報のクリアテキスト送信の脆弱性(06/24)
https://us-cert.cisa.gov/ics/advisories/icsma-21-175-01

・JTEKT の TOYOPUC PLC にはメモリバッファ境界内での操作の不適切な制限の脆弱性(07/01)
https://us-cert.cisa.gov/ics/advisories/icsa-21-180-04

・Delta Electronics の DOPSoft には範囲外読み取りの脆弱性(07/01)
https://us-cert.cisa.gov/ics/advisories/icsa-21-182-03
※CVSSv3 では基本値「7.8」となっています。

・VISAM の VBASE に複数の脆弱性(更新)(07/08)
https://us-cert.cisa.gov/ics/advisories/icsa-20-084-01
※CVSSv3 では基本値「9.0」となっています。

（２）その他
・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(米国 CERT/CC)(06/24)
https://kb.cert.org/vuls/id/799380

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７月２７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。