ＮＩＳＣ重要インフラニュースレター第２９５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２９５号（１０／１２）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１０月１２日発行 第２９５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２９５号の目次　◆――――――――――――――――――――――――――┐

├――┤

○今号は、９月２８日～１０月１１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）Apache Software Foundation 製品に関する脆弱性

・Apache HTTP Server の脆弱性(CVE-2021-41773, CVE-2021-42013)に関する注意喚起(JPCERT/CC、IPA、JVN、米国 DHS)(10/06、10/07、10/08)

https://www.jpcert.or.jp/at/2021/at210043.html

https://www.ipa.go.jp/security/ciadr/vul/alert20211006.html

https://jvn.jp/jp/JVN51106450/

※CVSSv3 では基本値「7.5」となっています。

https://us-cert.cisa.gov/ncas/current-activity/2021/10/07/apache-releases-http-server-version-2451-address-vulnerabilities

（２）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(Google)(10/07)

https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html

（３）Mozilla 製品に関する脆弱性

・Mozilla が Firefox 及び FirefoxESR のセキュリティアップデートをリリース(米国 DHS)(10/06)

https://us-cert.cisa.gov/ncas/current-activity/2021/10/06/mozilla-releases-security-updates-firefox-and-firefox-esr

（４）その他

・CyberNewsFlash「Hikvision 製ネットワークカメラの脆弱性(CVE-2021-36260)について」(JPCERT/CC)(09/30)

https://www.jpcert.or.jp/newsflash/2021093001.html

・SonicWall 製の SMA100 シリーズの脆弱性(CVE-2021-20034)に関する注意喚起(JPCERT/CC、IPA)(10/01)

https://www.jpcert.or.jp/at/2021/at210042.html

https://www.ipa.go.jp/security/ciadr/vul/alert20211001.html

・WordPress 用プラグイン OG Tags 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)(09/28)
https://jvn.jp/jp/JVN29428319/

・スマートフォンアプリ「InBody」における情報漏えいの脆弱性(JVN)(09/28)
https://jvn.jp/jp/JVN63023305/

・iOS アプリ「スニーカーダンク スニーカーフリマアプリ」におけるサーバー証明書の検証不備の脆弱性(JVN)(09/28)
https://jvn.jp/jp/JVN10168753/

・トレンドマイクロ製スマートホームスキャナー(Windows 版)における権限昇格の脆弱性(JVN)(09/29)
https://jvn.jp/vu/JVNVU99718667/

・トレンドマイクロ製 ServerProtect における認証回避の脆弱性(JVN)(09/30)
https://jvn.jp/vu/JVNVU99520559/

・サイボウズ リモートサービスにおける複数の脆弱性(JVN)(09/30)
https://jvn.jp/jp/JVN52694228/

・Boston Scientific 製 ZOOM LATITUDE における複数の脆弱性(JVN)(10/01)
https://jvn.jp/vu/JVNVU95979327/

・Salesforce Developer Experience Command Line Interface におけるアクセス制限不備の問題(JVN)(10/05)
https://jvn.jp/vu/JVNVU97731134/

・三菱電機製 GOT およびテンションコントローラの TCP/IP プロトコルスタックにおける複数の脆弱性(JVN)(10/05)
https://jvn.jp/vu/JVNVU99532713/
※CVSSv3 では基本値「7.5」となっています。

・三菱電機製 MELSEC iQ-R シリーズ C 言語コントローラユニットにおけるリソース枯渇の脆弱性(JVN)(10/07)

https://jvn.jp/vu/JVNVU94914666/

・Emerson 製 WirelessHART Gateway における複数の脆弱性(JVN)(10/06)
https://jvn.jp/vu/JVNVU96051696/
※CVSSv3 では基本値「8.0」となっています。

・Moxa 製 MXview Network Management Software における複数の脆弱性(JVN)(10/06)
https://jvn.jp/vu/JVNVU91384521/
※CVSSv3 では基本値「10.0」となっています。

・Honeywell 製 Experion PKS における複数の脆弱性(JVN)(10/06)
https://jvn.jp/vu/JVNVU92081667/
※CVSSv3 では基本値「10.0」となっています。

・スマートフォンアプリ「Nike」における Custom URL Scheme の処理にアクセス制限不備の脆弱性(JVN)(10/08)
https://jvn.jp/jp/JVN89126639/

・Exacq Technologies 製 exacqVision に複数の脆弱性(JVN)(10/08)
https://jvn.jp/vu/JVNVU97701389/
※CVSSv3 では基本値「9.8」となっています。

・複数の Mobile Industrial Robots 製品における複数の脆弱性(JVN)(10/08)
https://jvn.jp/vu/JVNVU93417317/
※CVSSv3 では基本値「9.8」となっています。

・InHand Networks 製ルーターIR615 に複数の脆弱性(JVN)(10/08)
https://jvn.jp/vu/JVNVU94119363/
※CVSSv3 では基本値「9.8」となっています。

・複数の FATEK Automation 製品に複数の脆弱性(JVN)(10/08)
https://jvn.jp/vu/JVNVU93626160/
※CVSSv3 では基本値「9.8」となっています。

２．政府機関の動き

● 総務省

・「クラウドサービス提供における情報セキュリティ対策ガイドライン(第３版)」(案)に対する意見募集の結果及び「クラウドサービス提供における情報セキュリティ対策ガイドライン(第３版)」の公表(09/30)
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html

・電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第四次とりまとめ(案)についての意見募集(10/05)
https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000130.html

３．関係機関の動き

（１）ＩＰＡ

・Java 実行環境を再構築した STAMP Workbench Ver.2.0.0 を公開(09/30)
https://www.ipa.go.jp/sec/tools/stamp_workbench.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・JPCERT/CC Eyes「攻撃グループ BlackTech が使用するマルウェア Gh0stTimes」(09/28)
https://blogs.jpcert.or.jp/ja/2021/09/gh0sttimes.html

・Weekly Report 2021-09-29 号(09/29)
https://www.jpcert.or.jp/wr/2021/wr213801.html

・Weekly Report 2021-10-06 号(10/06)
https://www.jpcert.or.jp/wr/2021/wr213901.html

４．海外の動き

● 米国 DHS

・CISA 及び NSA が VPN の選択と強化に関するガイダンスをリリース(09/28)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/28/cisa-and-nsa-release-guidance-selecting-and-hardening-vpns

・サイバーセキュリティ啓発月間でサイバースマートになる(10/05)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/05/be-cyber-smart-during-cybersecurity-awareness-month

・CISA がガイダンスをリリース：TIC3.0 リモートユーザーのユースケース(10/07)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/07/cisa-releases-guidance-tic-30-remote-user-use-case

・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(10/07)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/07/cisco-releases-security-updates-multiple-products

・NSA は、Wildcard TLS 証明書及び ALPACA 技術の危険を回避するためのガイダンスをリリース(10/08)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/08/nsa-releases-guidance-avoiding-dangers-wildcard-tls-certificates

・2021 年 9 月 27 日の週の脆弱性概報(10/04)
https://us-cert.cisa.gov/ncas/bulletins/sb21-277

・2021 年 10 月 4 日の週の脆弱性概報(10／11)
https://us-cert.cisa.gov/ncas/bulletins/sb21-284

・Microsoft Windows の Active Directory 証明書サービスは、PetitPotamNTLM リレー攻撃による AD の侵害の脆弱性(更新)(10/05)
https://kb.cert.org/vuls/id/405600

・Dnsmasq はメモリ破損やキャッシュポイズニングに脆弱(更新)(10/06)
https://kb.cert.org/vuls/id/434904

・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)(10/07)

https://kb.cert.org/vuls/id/914124

・Medtronic が MiniMed MMT-500 及び MMT-503 リモートコントローラーにキャプチャリプレイによる認証バイパス等の脆弱性(更新)(10/05)
https://us-cert.cisa.gov/ics/advisories/ICSMA-18-219-02

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１０月２６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。