ＮＩＳＣ重要インフラニュースレター第２９４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２９４号（9／２８）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２８日発行 第２９４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２９４号の目次　◆――――――――――――――――――――――――――┐

├――┤
○今号は、９月１４日～９月２７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 製品の脆弱性対策について(2021 年 9 月)(米国 DHS、IPA、JPCERT/CC)(09/14、09/15、09/17)

https://us-cert.cisa.gov/ncas/current-activity/2021/09/14/microsoft-releases-september-2021-security-updates

https://www.ipa.go.jp/security/ciadr/vul/20210915-ms.html

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

https://www.jpcert.or.jp/at/2021/at210041.html

（２）Adobe 製品に関する脆弱性

・Adobe Acrobat および Reader の脆弱性対策について(APSB21-55)(CVE-2021-39863 等)(米国 DHS、IPA、JPCERT/CC)(09/14、09/15)

https://us-cert.cisa.gov/ncas/current-activity/2021/09/14/adobe-releases-security-updates-multiple-products

https://www.ipa.go.jp/security/ciadr/vul/20210915-adobereader.html

https://www.jpcert.or.jp/at/2021/at210040.html

https://www.jpcert.or.jp/newsflash/2021091501.html

（３）Google 製品に関する脆弱性

・Google が Chrome のセキュリティアップデートをリリース(米国 DHS)(09/24)

https://us-cert.cisa.gov/ncas/current-activity/2021/09/24/google-releases-security-updates-chrome

（４）VMware がセキュリティアップデートをリリース(米国 DHS)(09/21、09/24)

https://us-cert.cisa.gov/ncas/current-activity/2021/09/21/vmware-releases-security-updates

https://us-cert.cisa.gov/ncas/current-activity/2021/09/24/vmware-vcenter-server-vulnerability-cve-2021-22005-under-active

（５）その他

・Siemens 製品に対するアップデート(2021 年 9 月)(JVN)(09/15)

https://jvn.jp/vu/JVNVU96712416/

・Digi International 製 PortServer TS 16 における不適切な認証の脆弱性(JVN)(09/15)
https://jvn.jp/vu/JVNVU90903314/
※CVSSv3 では基本値「9.6」となっています。

・Sensormatic Electronics 製 KT-1 に認証回避の脆弱性(JVN)(09/15)
https://jvn.jp/vu/JVNVU99211731/
※CVSSv3 では基本値「8.6」となっています。

・Schneider Electric 製 StruxureWare Data Center Expert における複数の脆弱性(JVN)(09/15)
https://jvn.jp/vu/JVNVU90520782/
※CVSSv3 では基本値「9.1」となっています。

・Schneider Electric 製 EcoStruxure および SCADAPack におけるディレクトリトラバーサルの脆弱性(JVN)(09/21)
https://jvn.jp/vu/JVNVU98742301/
※CVSSv3 では基本値「7.8」となっています。

・Apache Tomcat におけるサービス運用妨害(DoS)の脆弱性(JVN)(09/16)
https://jvn.jp/vu/JVNVU92089088/

・EC-CUBE 用プラグイン「注文ステータス一括変更プラグイン」におけるクロスサイトスクリプティングの脆弱性(JVN)(09/16)
https://jvn.jp/jp/JVN23406150/

・シャープ NEC ディスプレイソリューションズ製パブリックディスプレイにおける複数の脆弱性(JVN)(09/17)
https://jvn.jp/jp/JVN42866574/
※CVSSv3 では基本値「10.0」となっています。

・複数の Trane 製品におけるコードインジェクションの脆弱性(JVN)(09/24)
https://jvn.jp/vu/JVNVU93761221/
※CVSSv3 では基本値「9.9」となっています。

・CyberNewsFlash「Apple 製品のアップデートについて(2021 年 9 月)」(JPCERT/CC)(09/24)
https://www.jpcert.or.jp/newsflash/2021091401.html

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 31 回会合を開催(09/27)
https://www.nisc.go.jp/conference/cs/index.html#cs31

・新たなサイバーセキュリティ戦略が閣議決定されました(09/28)
https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf

（２）警察庁

・ランサムウェア被害防止対策の更新について(09/16)
https://www.npa.go.jp/cyber/ransom/index.html

３．関係機関の動き

（１）ＩＰＡ

・「情報セキュリティサービス基準適合サービスリスト」にサービスを追加しました。(09/22)
https://www.ipa.go.jp/security/it-service/service_list.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2021-09-15 号(09/15)
https://www.jpcert.or.jp/wr/2021/wr213601.html

・Weekly Report 2021-09-24 号(09/24)
https://www.jpcert.or.jp/wr/2021/wr213701.html

┃４．海外の動き

┼──┼

● 米国 DHS

・CISA、FBI 及び NSA が共同でランサムウェア Conti に関するサイバーセキュリティアドバイザリをリリース?(09/22)

https://us-cert.cisa.gov/ncas/current-activity/2021/09/22/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-conti

https://us-cert.cisa.gov/ncas/alerts/aa21-265a

・FBI-CISA-CGCYBER が Zoho ManageEngine ADSelfServicePlus の脆弱性の APT 活用に関するアドバイザリ(09/16)

https://us-cert.cisa.gov/ncas/current-activity/2021/09/16/fbi-cisa-cgcyber-advisory-apt-exploitation-manageengine

・Siemens の JT2Go 及び Teamcenter Visualization に範囲外の書き込み等の脆弱性(更新)(09/14)

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-03

※CVSSv3 では基本値「7.8」となっています。

・Siemens の SIMATIC S7-1200 に不適切な認証の脆弱性(更新)(09/14)

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-09

※CVSSv3 では基本値「8.1」となっています。

・Siemens の PROFINET Devices に制限や調整なしのリソースの割り当ての脆弱性(更新)(09/14)

https://us-cert.cisa.gov/ics/advisories/icsa-21-194-03

※CVSSv3 では基本値「7.5」となっています。

・Siemens の SIMATIC ソフトウェア製品に重要なリソースに対する不正なアクセス許可の割り当ての脆弱性(更新)(09/14)

https://us-cert.cisa.gov/ics/advisories/icsa-21-194-06

※CVSSv3 では基本値「7.3」となっています。

・Siemens の SINAMICS PERFECT HARMONY GH180 にメモリバッファの範囲内での操作の不適切な制限の脆弱性(更新)(09/14)

https://us-cert.cisa.gov/ics/advisories/icsa-21-194-13
※CVSSv3 では基本値「8.1」となっています。

・Siemens の SINUMERIK ONE 及び SINUMERIK MC にメモリバッファの範囲内での操作の不適切な制限の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-17
※CVSSv3 では基本値「8.1」となっています。

・Siemens の SIMATIC S7-1200 及び S7-1500 CPU Families にメモリバッファの範囲内での操作の不適切な制限の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-152-01
※CVSSv3 では基本値「8.1」となっています。

・Siemens の Linux ベース製品に不十分な乱数値使用の脆弱性(更新) (09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-03
※CVSSv3 では基本値「7.4」となっています。

・Siemens の SIMATIC SmartVNC HMI WinCC にバッファ CWE-788 の終了後のメモリ位置へのアクセス等の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-12
※CVSSv3 では基本値「9.8」となっています。

・Siemens の Web Server of SCALANCE X200 にヒープベースのバッファオーバーフロー等の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-07
※CVSSv3 では基本値「9.8」となっています。

・Siemens の SCALANCE 及び SIMATIC libcurl に範囲外の読み取りの脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-10
※CVSSv3 では基本値「7.5」となっています。

・Siemens の TIA Administrato に不適切なアクセス制御の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-05
※CVSSv3 では基本値「7.8」となっています。

・Siemens の SCALANCE X スイッチにハードコードされた暗号化キーの使用の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-02
※CVSSv3 では基本値「9.1」となっています。

・Siemens の SCALANCE X 製品にヒープ ベースのバッファ オーバーフロー認証欠落の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-05
※CVSSv3 では基本値「9.8」となっています。

・Siemens の SIMATIC、SINAMICS、SINEC、SINEMA 及び SINUMERIK に引用符で囲まれていないプログラムパスの脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-04

・Siemens の SCALANCE 及び SIMATIC にリソース枯渇の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-07
※CVSSv3 では基本値「7.5」となっています。

・Siemens の産業オートメーション機器に整数オーバーフロー等の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-19-253-03
※CVSSv3 では基本値「7.5」となっています。

・Siemens の SCALANCE X スイッチに不十分なリソース確保の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-19-225-03
※CVSSv3 では基本値「8.6」となっています。

・三菱電機の MELSEC iQ-R Series にリソース枯渇の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-20-324-05
※CVSSv3 では基本値「7.5」となっています。

・Johnson Controls Sensormatic Electronics の KT-1 にキャプチャリプレイによる認証バイパスの脆弱性(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-02-0

※CVSSv3 では基本値「8.6」となっています。

・CERT NZ が企業向けのランサムウェア保護ガイドをリリース(09/14)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/14/cert-nz-releases-ransomware-protection-guide-businesses

・SAP が 2021 年 9 月にセキュリティアップデートをリリース(09/14)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/14/sap-releases-september-2021-security-updates

・Citrix が ShareFileStorage ZonesController のセキュリティアップデートをリリース(09/14)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/14/citrix-releases-security-update-sharefile-storage-zones-controller

・HCC Embedded の InterNiche TCP/IP stack 及び NicheLite に複数の脆弱性(更新)(09/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-217-01
※CVSSv3 では基本値「9.8」となっています。

・Microsoft が AzureLinux Open Management Infrastructure のセキュリティ更新プログラムをリリース(米国 DHS)(09/16)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/16/microsoft-releases-security-update-azure-linux-open-management

・ManageEngine ADSelfServicePlus で新たに特定された脆弱性を悪用する APT アクター(09/16)
https://us-cert.cisa.gov/ncas/alerts/aa21-259a

・Drupal が複数製品のセキュリティアップデートをリリース(09/16)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/16/drupal-releases-multiple-security-updates

・オーストラリアサイバーセキュリティセンター(ACSC)が 2020?2021 年のサイバー脅威レポートをリリース(09/16)

https://us-cert.cisa.gov/ncas/current-activity/2021/09/16/acsc-releases-annual-cyber-threat-report

・2021 年 9 月 13 日の週の脆弱性概報(09/20)
https://us-cert.cisa.gov/ncas/bulletins/sb21-263

・2021 年 9 月 20 日の週の脆弱性概報(09/27)
https://us-cert.cisa.gov/ncas/bulletins/sb21-270

・NETGEAR がリモートコード実行の脆弱性に関するセキュリティアップデートをリリース(09/21)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/21/netgear-releases-security-updates-rce-vulnerability

・CISA リリースガイダンス：TIC3.0 の IPv6 に関する考慮事項(09/23)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/23/cisa-releases-guidance-ipv6-considerations-tic-30

・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(09/23)
https://us-cert.cisa.gov/ncas/current-activity/2021/09/23/cisco-releases-security-updates-multiple-products

・Ovarro の TBox にコードインジェクション等の脆弱性(更新)(09/23)
https://us-cert.cisa.gov/ics/advisories/icsa-21-054-04
※CVSSv3 では基本値「8.8」となっています。

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１２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。