ＮＩＳＣ重要インフラニュースレター第 288 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 288 号（6/22）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６月２２日発行 第２８８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２８８号の目次　◆――――――――――――――――――――――――――――┐

├――┤
○今号は、６月８日～６月２１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 は 2021 年 6 月のセキュリティアップデートをリリース(米国 DHS、IPA、JPCERT/CC)(06/08、06/09)

https://us-cert.cisa.gov/ncas/current-activity/2021/06/08/microsoft-releases-june-2021-security-updates

https://www.ipa.go.jp/security/ciadr/vul/20210609-ms.html

https://www.jpcert.or.jp/at/2021/at210027.html

（２）Adobe 製品に関する脆弱性

・Adobe は複数製品のセキュリティアップデートをリリース(米国 DHS、IPA、JPCERT/CC) (06/08、06/09)

https://us-cert.cisa.gov/ncas/current-activity/2021/06/08/adobe-releases-security-updates-multiple-products

https://www.ipa.go.jp/security/ciadr/vul/20210609-adobereader.html

https://www.jpcert.or.jp/at/2021/at210026.html

https://www.jpcert.or.jp/newsflash/2021060901.html

（３）Google 製品(Chrome)に関する脆弱性

・Google は Chrome のセキュリティアップデートをリリース(米国 DHS)(06/10、06/18)

https://us-cert.cisa.gov/ncas/current-activity/2021/06/10/google-releases-security-updates-chrome

https://us-cert.cisa.gov/ncas/current-activity/2021/06/18/google-releases-security-updates-chrome

（４）その他

・Intel 製品に関する複数の脆弱性について(2021 年 6 月)(JPCERT/CC、JVN)(06/09、06/10)

https://www.jpcert.or.jp/newsflash/2021060902.html

https://jvn.jp/vu/JVNVU99965981/

・トレンドマイクロ製ウイルスバスター for Home Network における複数の脆弱性(JVN)(06/09)
https://jvn.jp/vu/JVNVU92417259

・Rockwell Automation 製 ISaGRAF5 Runtime に複数の脆弱性(JVN)(06/09)
https://jvn.jp/vu/JVNVU90811375/
※CVSSv3 では基本値「9.1」となっています。

・Rockwell Automation 製 FactoryTalk Services Platform に保護メカニズムの不備の脆弱性(JVN)(06/11)
https://jvn.jp/vu/JVNVU90524470/

・AVEVA Software 製 InTouch にメモリ内の機微な情報が平文保存される脆弱性(JVN)(06/09)
https://jvn.jp/vu/JVNVU94212650/

・Johnson Controls 製 Metasys Servers、Engines、SCT Tools に不適切な権限管理の脆弱性(JVN)(06/09)
https://jvn.jp/vu/JVNVU91693325/
※CVSSv3 では基本値「8.8」となっています。

・Thales 製 Sentinel LDK Run-Time Environment における不十分なアンインストール処理の脆弱性(JVN)(06/09)
https://jvn.jp/vu/JVNVU95634783/
※CVSSv3 では基本値「9.6」となっています。

・複数の Schneider Electric 製品における脆弱性(JVN)(06/09)
https://jvn.jp/vu/JVNVU94079949/
※CVSSv3 では基本値「7.8」となっています。

・Schneider Electric 製 Enerlin'X Com'X 510 に不適切な権限管理の脆弱性(JVN)(06/18)
https://jvn.jp/vu/JVNVU93458321/
※CVSSv3 では基本値「8.5」となっています。

・Open Design Alliance 製 Drawings SDK における複数の脆弱性(JVN)(06/09)
https://jvn.jp/vu/JVNVU95145431/
※CVSSv3 では基本値「7.8」となっています。

・Siemens 製品に対するアップデート（2021 年 6 月)(JVN)(06/09)
https://jvn.jp/vu/JVNVU95781418/

・ZOLL 製 Defibrillator Dashboard における複数の脆弱性(JVN)(06/11)
https://jvn.jp/vu/JVNVU99848546/
※CVSSv3 では基本値「9.9」となっています。

・AGG Software 製 Web Server Plugin に複数の脆弱性(JVN)(06/11)
https://jvn.jp/vu/JVNVU95074675/
※CVSSv3 では基本値「8.2」となっています。

・WordPress 用プラグイン Welcart e-Commerce におけるクロスサイトスクリプティングの脆弱性(JVN)(06/11)
https://jvn.jp/jp/JVN70566757/

・GROWI における複数の脆弱性(JVN)(06/14)
https://jvn.jp/jp/JVN95457785/
※CVSSv3 では基本値「7.5」となっています。

・Android アプリ「あすけん」におけるアクセス制限不備の脆弱性(JVN)(06/14)
https://jvn.jp/jp/JVN38034268/

・Apache HTTP Web Server2.4 における複数の脆弱性に対するアップデート(JVN)(06/14)
https://jvn.jp/vu/JVNVU96037838/

・複数の ETUNA 製 EC-CUBE 用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)(06/15)
https://jvn.jp/jp/JVN79254445/

・複数の EC-CUBE 3.0 系用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に関する注意喚起(JPCERT/CC)(06/15)
https://www.jpcert.or.jp/at/2021/at210028.html

・複数の EC-CUBE 製 EC-CUBE 用プラグイン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)(06/15)
https://jvn.jp/jp/JVN57524494/
※CVSSv3 では基本値「7.1」となっています。

・ThroughTek 製 P2P SDK に重要な情報の平文での送信の脆弱性(JVN)(06/16)
https://jvn.jp/vu/JVNVU91747873/
※CVSSv3 では基本値「9.1」となっています。

・Automation Direct 製 CLICK PLC CPU Modules に複数の脆弱性(JVN)(06/16)
https://jvn.jp/vu/JVNVU94696836/
※CVSSv3 では基本値「9.8」となっています。

・Hitachi Application Server ヘルプにおけるクロスサイトスクリプティングの脆弱性(JVN)(06/17)
https://jvn.jp/jp/JVN03776901/

・日立仮想ファイルプラットフォーム製品における OS コマンドインジェクションの脆弱性(JVN)(06/18)
https://jvn.jp/jp/JVN21298724/
※CVSSv3 では基本値「8.8」となっています。

・Advantech 製 WebAccess/SCADA における複数の脆弱性(JVN)(06/18)
https://jvn.jp/vu/JVNVU91695634/
※CVSSv3 では基本値「7.3」となっています。

・Softing 製 OPC-UA C++ SDK にバッファエラーの脆弱性(JVN)(06/18)
https://jvn.jp/vu/JVNVU95863438/
※CVSSv3 では基本値「7.5」となっています。

□━━━■

┃２．政府機関の動き

┼──────────────────────────────────────┼

（１）ＮＩＳＣ

・「政府機関・地方公共団体等における業務での LINE 利用状況調査を踏まえた今後の LINE サービス等の利用の際の考え方（ガイドライン）」の一部改正(06/11)

https://www.nisc.go.jp/active/general/pdf/guideline210611.pdf

（２）総務省

・「ICT サイバーセキュリティ総合対策 2021」（案）に対する意見募集(06/09)

https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00189.html

・サイバーセキュリティタスクフォース（第 32 回）(6/3 開催)(06/11)

https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00190.html

■──────────────────────────────────────□

┃３．関係機関の動き

┼──────────────────────────────────────┼

● ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2021-06-09 号(06/09)

https://www.jpcert.or.jp/wr/2021/wr212201.html

・Weekly Report 2021-06-16 号(06/16)

https://www.jpcert.or.jp/wr/2021/wr212301.html

□──────────────────────────────────────■

┃４．海外の動き

┼──────────────────────────────────────┼

● 米国 DHS

・SAP は 2021 年 6 月のセキュリティアップデートをリリース(06/08)

https://us-cert.cisa.gov/ncas/current-activity/2021/06/08/sap-releases-june-2021-security-updates

・Thales の Sentinel LDK Run-Time 環境に不完全なクリーンアップの脆弱性(06/08)

https://us-cert.cisa.gov/ics/advisories/icsa-21-159-06
※CVSSv3 では基本値「9.6」となっています。

・Siemens の PROFINET DCP を実装した機器に不適切な入力検証の脆弱性(更新)(06/08)
https://us-cert.cisa.gov/ics/advisories/ICSA-17-129-02

・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)(06/08)
https://us-cert.cisa.gov/ics/advisories/ICSA-17-339-01
※CVSSv3 では基本値「7.5」となっています。

・Siemens のイーサネット機器に適切でないリソース消費制限の脆弱性(更新)(06/08)
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-02
※CVSSv3 では基本値「7.5」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)(06/08)
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-04

・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)(06/08)
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-07

・Siemens の SIMATIC HMI に過度の認証試行の不適切な制限の脆弱性(更新)(06/08)
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-06

・Siemens の Solid Edge に範囲外の書き込みの脆弱性(更新)(06/08)
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-06
※CVSSv3 では基本値「7.8」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) (06/08)
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 SINAMICS 中電圧製品にメモリバッファの境界内での操作の不適切な制限の脆弱性(更新)(06/09)
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-04
※CVSSv3 では基本値「9.8」となっています。

・Rockwell Automation の ISaGRAF5 Runtime に相対パストラバーサルの脆弱性(06/08)
https://us-cert.cisa.gov/ics/advisories/icsa-20-280-01
※CVSSv3 では基本値「9.1」となっています。

・Rockwell Automation の ISaGRAF5 Runtime に相対パストラバーサルの脆弱性(更新)(06/17)
https://us-cert.cisa.gov/ics/advisories/icsa-20-280-01
※CVSSv3 では基本値「9.1」となっています。

・Schneider Electric の Modicon X80 に不許可の者への機密情報公開の脆弱性(06/08)
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-05

・Schneider Electric の IGSS に範囲外の書き込みの脆弱性(06/08)
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-04
※CVSSv3 では基本値「7.8」となっています。

・Schneider Electric の Enerlin'X Com'X 510 に不適切な特権管理の脆弱性(06/17)
https://us-cert.cisa.gov/ics/advisories/icsa-21-168-01
※CVSSv3 では基本値「8.5」となっています。

・AVEVA の InTouch にメモリ内の機密情報のクリア テキストストレージの脆弱性(06/08)
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-03

・Open Design Alliance の Drawings SDK に範囲外読み取りの脆弱性(06/08)
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-02
※CVSSv3 では基本値「7.8」となっています。

・Johnson Controls の Metasys に不適切な特権管理の脆弱性(06/08)

https://us-cert.cisa.gov/ics/advisories/icsa-21-159-01
※CVSSv3 では基本値「8.8」となっています。

・CISA は運用技術資産をターゲットにしたランサムウェアの増加に対処(06/09)
https://us-cert.cisa.gov/ncas/current-activity/2021/06/09/cisa-addresses-rise-ransomware-targeting-operational-technology

・2021 年 6 月 7 日の週の脆弱性概報(06/14)
https://us-cert.cisa.gov/ncas/bulletins/sb21-165

・2021 年 6 月 14 日の週の脆弱性概報(06/21)
https://us-cert.cisa.gov/ncas/bulletins/sb21-172

・OpenClinic GA に複数の脆弱性(更新)(06/15)
https://us-cert.cisa.gov/ics/advisories/icsma-20-184-01
※CVSSv3 では基本値「9.8」となっています。

・M&M ソフトウェアの fdtCONTAINER に信頼されていないデータの逆シリアル化の脆弱性(更新)(06/17)
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-05
※CVSSv3 では基本値「7.3」となっています。

・Advantech の WebAccess/SCADA に相対パストラバーサルの脆弱性(06/17)
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。

・Softing の OPC-UA C++ SDK にメモリバッファの境界内での操作の不適切な制限の脆弱性(06/17)
https://us-cert.cisa.gov/ics/advisories/icsa-21-168-02
※CVSSv3 では基本値「7.5」となっています。

・Cisco は複数製品のセキュリティアップデートをリリース(06/17)
https://us-cert.cisa.gov/ncas/current-activity/2021/06/17/cisco-releases-security-updates-multiple-products

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１３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。