ＮＩＳＣ重要インフラニュースレター第２８６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 286 号（5/25）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5月２５日発行 第２８６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２８６号の目次　◆――――――――――――――――――――――――――――┐

├――┤

○今号は、５月１１日～５月２４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 5 月のセキュリティアップデートをリリース(05/11、05/12)(米国 DHS、IPA、JPCERT/CC)

https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/microsoft-releases-may-2021-security-updates

https://www.ipa.go.jp/security/ciadr/vul/20210512-ms.html

https://www.jpcert.or.jp/at/2021/at210024.html

（２）Acrobat 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)(JPCERT/CC)(05/11、05/12)

https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/adobe-releases-security-updates-multiple-products

https://www.jpcert.or.jp/newsflash/2021051201.html

・Adobe Acrobat および Reader の脆弱性対策について(APSB21-29)(CVE-2021-28550 等)(IPA、JPCERT/CC)(05/12)

https://www.ipa.go.jp/security/ciadr/vul/20210512-adobereader.html

https://www.jpcert.or.jp/at/2021/at210023.html

（３）その他

・三菱電機製 GOT 及びテンションコントローラの MODBUS/TCP スレーブ通信機能におけるサービス運用妨害(DoS)の脆弱性(JVN)(05/11)

https://jvn.jp/vu/JVNVU99895108/

・CyberNewsFlash「Intel 製品に関する複数の脆弱性について」(JPCERT/CC)(05/12)

https://www.jpcert.or.jp/newsflash/2021051202.html

・CyberNewsFlash「Boot Camp に関するアップデートについて」(JPCERT/CC)(05/19)

https://www.jpcert.or.jp/newsflash/2021051901.html

・オムロン製 CX-One にスタックベースのバッファオーバーフローの脆弱性(JVN)(05/13)
https://jvn.jp/vu/JVNVU90806326/
※CVSSv3 では基本値「7.8」となっています。

・KonaWiki2 における複数の脆弱性(JVN)(05/13)
https://jvn.jp/jp/JVN34232719/
※CVSSv3 では基本値「7.5」となっています。

・RFNTPS における OS コマンドインジェクションの脆弱性(JVN)(05/13)
https://jvn.jp/jp/JVN13076220/
※CVSSv3 では基本値「8.8」となっています。

・IEEE802.11 規格のフレームアグリゲーションやフラグメンテーションに関する複数の問題(FragAttack)(JVN)(05/13)
https://jvn.jp/vu/JVNVU93485736/

・Cisco Small Business Series Wireless Access Points における複数の脆弱性(JVN)(05/14)
https://jvn.jp/jp/JVN71263107/
※CVSSv3 では基本値「9.0」となっています。

・Rockwell Automation 製 Connected Components Workbench に複数の脆弱性(JVN)(05/14)
https://jvn.jp/vu/JVNVU95873084/
※CVSSv3 では基本値「8.6」となっています。

・Sensormatic Electronics 社製 American Dynamics Tyco AI に境界条件の判定の脆弱性(JVN)(05/14)
https://jvn.jp/vu/JVNVU98963695/
※CVSSv3 では基本値「7.8」となっています。

・OPC 製品における複数の脆弱性(JVN)(05/14)

https://jvn.jp/vu/JVNVU98588994/
※CVSSv3 では基本値「7.5」となっています。

・mod_auth_openidc におけるサービス運用妨害(DoS)の脆弱性(JVN)(05/14)
https://jvn.jp/jp/JVN49704918/
※CVSSv3 では基本値「7.5」となっています。

・Siemens 製品に対するアップデート(2021 年 5 月)(JVN)(05/18)
https://jvn.jp/vu/JVNVU91051134/

・Emerson 製 Rosemount X-STREAM に複数の脆弱性(JVN)(05/19)
https://jvn.jp/vu/JVNVU97128016/
※CVSSv3 では基本値「7.5」となっています。

・ScanSnap Manager のインストーラにおける DLL 読み込みに関する脆弱性(JVN)(05/21)
https://jvn.jp/jp/JVN65733194
※CVSSv3 では基本値「7.8」となっています。

・QND における権限昇格の脆弱性(JVN)(05/21)
https://jvn.jp/jp/JVN74686032/
※CVSSv3 では基本値「7.8」となっています。

・Overwolf インストーラにおける DLL 読み込みに関する脆弱性(JVN)(05/21)
https://jvn.jp/jp/JVN78254777/
※CVSSv3 では基本値「7.8」となっています。

・複数の PHP 工房製品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)(05/21)
https://jvn.jp/jp/JVN53910556/

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 28 回会合を開催(05/13)
https://www.nisc.go.jp/conference/cs/index.html#cs28

（２）総務省
・サイバーセキュリティタスクフォース（第 31 回）(5/13 開催)(05/18)

https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00183.html

３．関係機関の動き

（１）ＪＰＣＥＲＴ コーディネーションセンター
・Weekly Report 2021-05-12 号(05/12)
https://www.jpcert.or.jp/wr/2021/wr211801.html

・JPCERT/CC Eyes「Locked Shields 2021 参加記」(05/18)
https://blogs.jpcert.or.jp/ja/2021/05/locked-shields-2021.html

・Weekly Report 2021-05-19 号(05/19)
https://www.jpcert.or.jp/wr/2021/wr211901.html

・JPCERT/CC Eyes「仮想通貨マイニングツールの設置を狙った攻撃」(05/20)
https://blogs.jpcert.or.jp/ja/2021/05/xmrig.html

４．海外の動き

（１）米国 DHS
・CISA と FBI は DarkSide ランサムウェアに関する共同サイバーセキュリティ勧告をリリース(05/11、05/19)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/joint-cisa-fbi-cybersecurity-advisory-darkside-ransomware
https://us-cert.cisa.gov/ncas/current-activity/2021/05/19/update-cisa-fbi-joint-cybersecurity-advisory-darkside-ransomware

・DarkSide ランサムウェア:ランサムウェア攻撃によるビジネスの中断を防ぐためのベストプラクティス(05/12)
https://us-cert.cisa.gov/ncas/alerts/aa21-131a

・TightVNC を使用した Siemens 製品にヒープベースのバッファオーバーフローの脆弱性(更新)(05/11)
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-08
※CVSSv3 では基本値「9.8」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)(05/11)
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 SIMARIS configuration に不正なデフォルトのアクセス許可の脆弱性(更新)(05/11)
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-08

・Siemens の SCALANCE 及び SIMATIC libcurl に範囲外の読み取りの脆弱性(更新)(05/11)
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 の組み込み TCP/IP スタックの脆弱性(AMNESIA:33)(更新)(05/11)
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-06

・三菱電機 GOT 及びテンションコントローラに範囲外の読み取りの脆弱性(更新)(05/13)
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-02
※CVSSv3 では基本値「7.5」となっています。

・三菱電機の複数製品に脆弱性(更新)(05/18)
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。

・三菱電機の MELSEC iQ-R Series にリソース枯渇の脆弱性(更新)(05/18)
https://us-cert.cisa.gov/ics/advisories/icsa-20-282-02
※CVSSv3 では基本値「8.6」となっています。
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。

・三菱電機の MELFA に制御されていないリソース枯渇の脆弱性(更新)(05/18)
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-04
※CVSSv3 では基本値「7.5」となっています。

・三菱電機の MELSEC iQ-R、Q 及び L Series に制御されていないリソース枯渇の脆弱性(更新)(05/19)
https://us-cert.cisa.gov/ics/advisories/icsa-20-303-01
※CVSSv3 では基本値「7.5」となっています。

・Juniper Networks はセキュリティアップデートをリリース(05/11)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/juniper-networks-releases-security-updates

・Citrix は Windows 用ワークスペースアプリケーションのセキュリティアップデートをリリース(05/11)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/citrix-releases-security-updates-workspace-app-windows

・WordPress はセキュリティアップデートをリリース(05/13)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/13/wordpress-releases-security-update

・CISA は SolarWinds 及びアクティブディレクトリ/M365 の侵害の影響を受けるネットワークからの侵入者排除のガイダンスを公開(05/14)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/14/cisa-publishes-eviction-guidance-networks-affected-solarwinds-and

・2021 年 5 月 10 日の週の脆弱性概報(05/17)

https://us-cert.cisa.gov/ncas/bulletins/sb21-137

・2021 年 5 月 17 日の週の脆弱性概報(05/24)
https://us-cert.cisa.gov/ncas/bulletins/sb21-144

・Cisco は複数製品のセキュリティアップデートをリリース(05/20)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/20/cisco-releases-security-updates-multiple-products

・複数の RTOS に整数オーバーフローまたはラップアラウンドの脆弱性(更新)(05/20)
https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04
※CVSSv3 では基本値「9.8」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６月８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。