■―――――――――――――――――――――――――――――――――□

┃　　◆◆　NISC 重要インフラニュースレター　◆◆

┃　　（２０１９年６月２５日発行 第２４０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２４０号の目次　◆―――――――――――――――――――――┐

├―――――――――――――――――――――――――――――――――――┤

○今号は、６月１１日～６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）Adobe 社製品に関する脆弱性

・Adobe Flash Player の脆弱性対策について(APSB19-30)(CVE-2019-7845)(IPA、JPCERT/CC)(06/12)

https://www.ipa.go.jp/security/ciadr/vul/20190612-adobeflashplayer.html

https://www.jpcert.or.jp/at/2019/at190025.html

・CyberNewsFlash「複数の Adobe 製品のアップデートについて」(06/12)

https://www.jpcert.or.jp/newsflash/2019061202.html

（２）Microsoft 社製品に関する脆弱性

・Microsoft 製品の脆弱性対策について(2019 年 6 月)(IPA、JPCERT/CC)(06/12)

https://www.ipa.go.jp/security/ciadr/vul/20190612-ms.html

https://www.jpcert.or.jp/at/2019/at190026.html

・CyberNewsFlash「リモートデスクトップサービスにおける脆弱性 CVE-2019-0708 について(追加情報)」(JPCERT/CC)(06/19)

https://www.jpcert.or.jp/newsflash/2019061901.html

（３）Oracle 社製品に関する脆弱性

・Oracle WebLogic Server の脆弱性（CVE-2019-2729）について(IPA、JPCERT/CC)(06/19)
https://www.ipa.go.jp/security/ciadr/vul/20190619_WebLogicServer.html
https://www.jpcert.or.jp/at/2019/at190028.html

（４）Intel 社製品に関する脆弱性

・Intel 製品に複数の脆弱性(JVN、JPCERT/CC)(06/12)
https://jvn.jp/vu/JVNVU95572531/index.html
https://www.jpcert.or.jp/newsflash/2019061201.html

（５）その他

・Firefox の脆弱性（CVE-2019-11707）に関する注意喚起（公開)(JPCERT/CC)(06/19)
https://www.jpcert.or.jp/at/2019/at190027.html

・WordPress 用プラグイン Contest Gallery 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)(06/12)
https://jvn.jp/jp/JVN80925867/index.html

・Apple iCloud for Windows における脆弱性に対するアップデート(JVN)(06/13)
https://jvn.jp/vu/JVNVU95342995/index.html

・WordPress 用プラグイン Related YouTube Videos 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)(06/17)
https://jvn.jp/jp/JVN31406910/index.html

・WordPress 用プラグイン Personalized WooCommerce Cart Page 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)(06/19)
https://jvn.jp/jp/JVN88804335/index.html

・ISC BIND 9 にサービス運用妨害（DoS）の脆弱性(JVN、JPCERT/CC)(06/20)
https://jvn.jp/vu/JVNVU90363752/index.html
https://www.jpcert.or.jp/newsflash/2019062001.html

・CyberNewsFlash「Mozilla 製品における脆弱性（CVE-2019-11708）について」(JPCERT/CC)(06/21)
https://www.jpcert.or.jp/newsflash/2019062101.html

・VAIO Update における複数の脆弱性(JVN)(06/21)
https://jvn.jp/jp/JVN13555032/index.html
※CVSSv3 では基本値「7.8」となっています。

・Linux および FreeBSD カーネルにおけるサービス運用妨害（DoS）の脆弱性(JVN)(06/21)
https://jvn.jp/vu/JVNVU93800789/index.html

・Apache Tomcat におけるサービス運用妨害（DoS）の脆弱性(JVN)(06/21)
https://jvn.jp/vu/JVNVU99826833/index.html
※CVSSv3 では基本値「7.5」となっています。

・WordPress 用プラグイン HTML5 Maps 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)(06/24)
https://jvn.jp/jp/JVN49575131/index.html

・WordPress 用プラグイン Custom CSS Pro 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)(06/24)
https://jvn.jp/jp/JVN29933378/index.html

・Apple AirPort Base Station における脆弱性に対するアップデート(JVN)(06/24)
https://jvn.jp/vu/JVNVU96755549/index.html

２．政府機関の動き

（１）警察庁
・リモートデスクトップサービスを標的としたアクセスの増加等について(06/21)
https://www.npa.go.jp/cyberpolice/important/2019/201906211.html

・平成 31 年 3 月期観測資料(06/21)
https://www.npa.go.jp/cyberpolice/important/2019/201906212.html

・平成 31 年 4 月期観測資料(06/21)
https://www.npa.go.jp/cyberpolice/important/2019/201906213.html

・令和元年 5 月期観測資料(06/21)
https://www.npa.go.jp/cyberpolice/important/2019/201906214.html

（２）金融庁
・「金融分野のサイバーセキュリティレポート」の公表について(06/21)
https://www.fsa.go.jp/news/30/20190621-cyber.html

・「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(06/21)
https://www.fsa.go.jp/news/30/20190621-1.html

・「クラウドコンピューティングとサイバーセキュリティ等に関する調査報告書」の公表について(06/11)
https://www.fsa.go.jp/common/about/research/20190611-2.html

（３）総務省
・サイバーセキュリティ人材育成分科会　第 1 次取りまとめ案に対する意見募集の結果及び第 1 次取りまとめの公表(06/14)
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00028.html

（４）経済産業省

・中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）の各事業を公開しました(06/11)

https://www.meti.go.jp/press/2019/06/20190611001/20190611001.html

・ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第１版を策定しました(06/17)

https://www.meti.go.jp/press/2019/06/20190617005/20190617005.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 2019-06-12 号(06/12)

https://www.jpcert.or.jp/wr/2019/wr192201.html

・Weekly Report 2019-06-19 号(06/19)

https://www.jpcert.or.jp/wr/2019/wr192301.html

４．海外の動き

● 米国 DHS

・Cisco 社がネットワーク ソフトウェアについてのセキュリティアップデートをリリース。(06/12)

https://www.us-cert.gov/ncas/current-activity/2019/06/12/Cisco-Releases-Security-Update-Cisco-IOS-XE

・米国連邦取引委員会（ＦＴＣ）が財務・税情報のような機微情報を保護するためにソフトウェアのアップデートを行うよう注意喚起を実施。(06/13)

https://www.us-cert.gov/ncas/current-activity/2019/06/13/FTC-Releases-Alert-Updating-Software

・Exim が Exim versions 4.87～4.91 についてのセキュリティパッチをリリース。(06/13)

https://www.us-cert.gov/ncas/current-activity/2019/06/13/Exim-Releases-Security-Patches

・Google が Chrome についてのセキュリティアップデートをリリース。(06/13)

https://www.us-cert.gov/ncas/current-activity/2019/06/13/Google-Releases-Security-Updates-Chrome

・Samba が Samba 4.9 以降についてのセキュリティアップデートをリリース。(06/19)

https://www.us-cert.gov/ncas/current-activity/2019/06/19/Samba-Releases-Security-Updates

・Cisco 社が複数の製品についてのセキュリティアップデートをリリース。(06/19)

https://www.us-cert.gov/ncas/current-activity/2019/06/19/Cisco-Releases-Security-Updates-Multiple-Products

・Mozilla が Firefox 及び Thunderbird についてのセキュリティアップデートをリリース。(06/20)
https://www.us-cert.gov/ncas/current-activity/2019/06/20/Mozilla-Releases-Security-Updates-Firefox-and-Firefox-ESR

・Microsoft 社が Android 用 Outlook についてのセキュリティアップデートをリリース。(06/20)
https://www.us-cert.gov/ncas/current-activity/2019/06/20/Microsoft-Releases-Outlook-Android-Security-Update

・Dell 社が Dell SupportAssist についての注意喚起を実施。(06/21)
https://www.us-cert.gov/ncas/current-activity/2019/06/21/Dell-Releases-Security-Advisory-Dell-SupportAssist

・６月１０日の週の脆弱性概報(06/17)
https://www.us-cert.gov/ncas/bulletins/SB19-168

・６月１７日の週の脆弱性概報(06/24)
https://www.us-cert.gov/ncas/bulletins/SB19-175

・Siemens 社のイーサネットスイッチに保存復元可能なパスワード保存の脆弱性。(06/11)
https://ics-cert.us-cert.gov/advisories/ICSA-19-162-04
※CVSSv3 では基本値「7.1」となっています。

・Siemens 社の配電盤用電源にセッション固定等の脆弱性。(06/11)
https://ics-cert.us-cert.gov/advisories/ICSA-19-162-03
※CVSSv3 では基本値「7.5」となっています。

・Siemens 社の光学リーダーに不適切な特権管理等の脆弱性。(06/11)
https://ics-cert.us-cert.gov/advisories/ICSA-19-162-02
※CVSSv3 では基本値「7.1」となっています。

・Siemens 社の録画管理システムに不適切な認証等の脆弱性。(06/11)
https://ics-cert.us-cert.gov/advisories/ICSA-19-162-01
※CVSSv3 では基本値「8.8」となっています。

・医療用画像通信規格「DICOM」における脆弱性。(06/11)
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-19-162-01

・WAGO 社のイーサネットスイッチに資格情報がハードコーディングされている問題等の脆弱性。(06/13)
https://ics-cert.us-cert.gov/advisories/ICSA-19-164-02
※CVSSv3 では基本値「9.8」となっています。

・Johnson Controls 社の録画管理システムに不適切な認証の脆弱性。(06/13)
https://ics-cert.us-cert.gov/advisories/ICSA-19-164-01

・Becton, Dickinson and Company 社の医療用輸液システムに不適切なアクセス制御等の脆弱性。(06/13)
https://ics-cert.us-cert.gov/advisories/ICSMA-19-164-01
※CVSSv3 では基本値「10.0」となっています。

・Phoenix Contact 社のオートメーション・ソフトウェアに領域外のメモリ参照等の脆弱性。(06/20)
https://ics-cert.us-cert.gov/advisories/ICSA-19-171-01
※CVSSv3 では基本値「7.8」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、７月９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。

- ni(　^s^)c