■―――――――――――――――――――――――――――――――――□

┃　　◆◆　NISC 重要インフラニュースレター　◆◆

┃　　（２０１９年５月２８日発行 第２３８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２３８号の目次　◆―――――――――――――――――――――┐

├―――――――――――――――――――――――――――――――――┤

○今号は、５月１４日～５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）Adobe 社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(APSB19-18)(CVE-2019-7829 等)(IPA、JPCERT/CC)(05/15)

https://www.ipa.go.jp/security/ciadr/vul/20190515-adobereader.html

https://www.jpcert.or.jp/at/2019/at190022.html

・Adobe Flash Player の脆弱性対策について(APSB19-26)(CVE-2019-7837)(IPA、JPCERT/CC) (05/15)

https://www.ipa.go.jp/security/ciadr/vul/20190515-adobeflashplayer.html

https://www.jpcert.or.jp/at/2019/at190021.html

・CyberNewsFlash「Adobe 製品のアップデート（APSB19-29）について」(JPCERT/CC) (05/15)

https://www.jpcert.or.jp/newsflash/2019051502.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 5 月)(IPA、JPCERT/CC)(05/15)

https://www.ipa.go.jp/security/ciadr/vul/20190515-ms.html

https://www.jpcert.or.jp/at/2019/at190023.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」(JPCERT/CC)(05/15)
https://www.jpcert.or.jp/newsflash/2019051501.html

・Microsoft Windows タスクスケジューラにおける権限昇格の脆弱性(JVN)(05/24)
https://jvn.jp/vu/JVNVU93881163/index.html

（３）Intel 社製品に関する脆弱性
・Intel 製品の複数の脆弱性（INTEL-SA-00213）に関する注意喚起(JPCERT/CC、JVN)(05/15)
https://www.jpcert.or.jp/at/2019/at190024.html
https://jvn.jp/vu/JVNVU92328381/index.html

・CyberNewsFlash「Intel 製品に関する複数の脆弱性について」(JPCERT/CC)(05/15)
https://www.jpcert.or.jp/newsflash/2019051503.html

（４）その他
・Cisco トラストアンカーモジュール（TAm）におけるコード検証不備および Cisco IOS XE Web UI におけるユーザ入力検証不備の脆弱性(JVN)(05/16)
https://jvn.jp/vu/JVNVU97735735/index.html
※CVSSv3 では基本値「7.2」となっています。

・Apache Camel における XML 外部実体参照（XXE）に関する脆弱性(JVN)(05/22)
https://jvn.jp/jp/JVN71498764/index.html

・WordPress 用プラグイン WP Open Graph 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)(05/23)
https://jvn.jp/jp/JVN33652328/index.html

・三菱電機製 MELSEC-Q シリーズ Ethernet インタフェースユニットにおけるサービス運用妨害(DoS)の脆弱性(JVN)(05/23)
https://jvn.jp/vu/JVNVU93268101/index.html
※CVSSv3 では基本値「7.5」となっています。

・Android アプリ「Tootdon for マストドン(Mastodon)」における SSL サーバ証明書の検証不備の脆弱性(JVN)(05/24)
https://jvn.jp/jp/JVN57806517/index.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 22 回会合を開催(05/23)
https://www.nisc.go.jp/conference/cs/index.html#cs22

・研究開発戦略専門調査会第 11 回、第 12 回会合を開催(4/26、5/17 開催)(05/28)
https://www.nisc.go.jp/conference/cs/kenkyu/index.html#kenkyu12

（２）総務省

・「サイバーセキュリティ対策情報開示の手引き（案）」に対する意見募集(05/17)
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00024.html

（３）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）の実施地域・事業者が決定しました(05/17)
https://www.meti.go.jp/press/2019/05/20190517002/20190517002.html

■――――――――――――――――――――――――――――――――――□

３．関係機関の動き

――――――――――――――――――――――――――――――――――――

（１）ＩＰＡ

・プレス発表　入退管理システムにおける情報セキュリティ対策要件チェックリストを公開(05/20)
https://www.ipa.go.jp/about/press/20190520.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2019-05-15 号(05/15)
https://www.jpcert.or.jp/wr/2019/wr191801.html

・Weekly Report 2019-05-22 号(05/22)
https://www.jpcert.or.jp/wr/2019/wr191901.html

・マルウエア TSCookie の設定情報を正常に読み込めないバグ（続報）(05/28)
https://blogs.jpcert.or.jp/ja/2019/05/tscookie-2.html

□――――――――――――――――――――――――――――――――――■

４．海外の動き

――――――――――――――――――――――――――――――――――――

● 米国 DHS

・Facebook 社が WhatsApp についてのセキュリティアップデートをリリース。(05/14)
https://www.us-cert.gov/ncas/current-activity/2019/05/14/Facebook-Releases-Security-Advisory-WhatsApp

・Samba がセキュリティアップデートをリリース。(05/14)
https://www.us-cert.gov/ncas/current-activity/2019/05/14/Samba-Releases-Security-Updates

・Vmware 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。(05/14)
https://www.us-cert.gov/ncas/current-activity/2019/05/14/VMware-Releases-Security-Updates

・Mozilla が Firefox についてのセキュリティアップデートをリリース。(05/21)
https://www.us-cert.gov/ncas/current-activity/2019/05/21/Mozilla-Releases-Security-Updates-Firefox

・セキュリティアドバイス：選挙システムの防護(05/21)
https://www.us-cert.gov/ncas/tips/ST19-001-0

・５月１３日の週の脆弱性概報(05/20)

https://www.us-cert.gov/ncas/bulletins/SB19-140

・５月２０日の週の脆弱性概報(05/27)
https://www.us-cert.gov/ncas/bulletins/SB19-147

・Siemens 社のオートメーションシステム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(05/14)
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-09

・Siemens 社のオートメーションシステムに SQL インジェクション等の脆弱性(05/14)
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-08
※CVSSv3 では基本値「9.1」となっています。

・Siemens 社のネットワークコンポーネントに情報漏洩等の脆弱性(05/14)
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-07
※CVSSv3 では基本値「9.8」となっています。

・Siemens 社のオートメーションシステムに不適切な入力検証の脆弱性(05/14)
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-06
※CVSSv3 では基本値「7.5」となっています。

・Siemens 社のオートメーションシステムに適切でないリソース消費制限の脆弱性(05/14)
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-05
※CVSSv3 では基本値「7.5」となっています。

・Siemens 社のロジックモジュールに重要な機能に対する認証の欠如等の脆弱性(05/14)
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-04
※CVSSv3 では基本値「9.4」となっています。

・Siemens 社の PLC プログラミングソフトに信頼できないデータのデシリアライゼーションの脆弱性(05/14)
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-03
※CVSSv3 では基本値「7.8」となっています。

・Siemens 社のオートメーションシステムに重要な機能に対する認証の欠如の脆弱性(05/14)
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-02-0
※CVSSv3 では基本値「9.8」となっています。

・オムロン社のネットワークコンフィグレータに信頼できない検索パスの脆弱性(05/14)
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-01
※CVSSv3 では基本値「7.3」となっています。

・富士電機のＦＡ危機に領域外のメモリ参照の脆弱性(05/16)
https://ics-cert.us-cert.gov/advisories/ICSA-19-136-02

・Schneider Electric 社のプロセスコントローラーに不十分なランダム値の使用の脆弱性(05/16)
https://ics-cert.us-cert.gov/advisories/ICSA-19-136-01

・三菱電機のイーサネットモジュールに適切でないリソース消費制限の脆弱性(05/21)

https://ics-cert.us-cert.gov/advisories/ICSA-19-141-02
※CVSSv3 では基本値「7.5」となっています。

・Computrols 社のビルディングオートメーションシステムにコマンドインジェクション等の脆弱性(05/21)
https://ics-cert.us-cert.gov/advisories/ICSA-19-141-01
※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、６月１１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