◆◆ NISC重要インフラニュースレター ◆◆

（２０１９年４月９日発行 第２３５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２３５号の目次 ◆

１．チェックが必要な情報
２．政府機関の動き
３．関係機関の動き
４．海外の動き
５．読者へのお願い
６．次回予告

○今号は、３月２６日～４月８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

・CyberNewsFlash「Apache Tomcat の脆弱性（CVE-2019-0199）について」を公開(JPCERT/CC)(03/26)
https://www.jpcert.or.jp/newsflash/2019032601.html

（２）Apple社製品に関する脆弱性

・複数の Apple 製品における脆弱性に対するアップデート(JVN)(03/26)
https://jvn.jp/vu/JVNVU93236010/index.html

（３）その他

・PowerActPro Master Agent Windows版におけるアクセス制限不備の脆弱性(JVN)(03/27)
https://jvn.jp/jp/JVN63981842/index.html

・Android アプリ「JR東日本 列車運行情報 プッシュ通知アプリ」が使用する API サーバにアクセス制限不備の脆弱性(JVN)(04/01)
https://jvn.jp/jp/JVN01119243/index.html

・GNU Wget におけるバッファオーバーフローの脆弱性(JVN)(04/03)
https://jvn.jp/jp/JVN25261088/index.html

※CVSSv3 では基本値「8.8」となっています。

・オムロン製 CX-One に解放済みメモリ使用（use-after-free）の脆弱性(JVN)(04/05)
https://jvn.jp/vu/JVNVU98267543/index.html

２．政府機関の動き

（１）ＮＩＳＣ

・サイバーセキュリティ基本法の一部を改正する法律の施行及び同法に基づくサイバーセキュリティ協議会の組織について(04/01)
https://www.nisc.go.jp/conference/cs/kyogikai/index.html

（２）警察庁

・ウェブメールクライアント「Internet Messaging Program」の脆弱性を有する機器に対するアクセスの増加等について(03/28)
https://www.npa.go.jp/cyberpolice/important/2019/201903281.html

・平成３１年１月期観測資料(03/28)
https://www.npa.go.jp/cyberpolice/important/2019/201903282.html

・平成３１年２月期観測資料(03/28)
https://www.npa.go.jp/cyberpolice/important/2019/201903283.html

（３）経済産業省

・「サイバーセキュリティ経営ガイドライン Ver.2.0 実践のためのプラクティス集」を策定しました(03/25)
https://www.meti.go.jp/press/2018/03/20190325001/20190325001.html

・改元に伴う企業等の情報システム改修等への対応(04/02)
https://www.meti.go.jp/policy/it_policy/kaigen/kaigen_taiou.html

３．関係機関の動き

（１）ＩＰＡ

・「組込み/IoT に関する動向調査」の調査結果を公開(03/27)
https://www.ipa.go.jp/ikc/reports/20190327.html

・「2018 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査」報告書についてを公開しました。(03/28)
https://www.ipa.go.jp/security/fy30/reports/sme/index.html

・ＷＡＦ読本補足資料「Web Application Firewall の導入に向けた検討項目」を公開(03/28)
https://www.ipa.go.jp/security/vuln/waf.html

・ゴールデンウィークにおける情報セキュリティに関する注意喚起(04/02)
https://www.ipa.go.jp/security/topics/alert20190402.html

（２）ＪＰＣＥＲＴ　コーディネーションセンター
・Weekly Report 2019-03-27 号(03/27)
https://www.jpcert.or.jp/wr/2019/wr191201.html

・Weekly Report 2019-04-03 号(04/03)
https://www.jpcert.or.jp/wr/2019/wr191301.html

・JPCERT/CC Eyes「メキシコ・ブラジルの CSIRT を訪ねて」(04/04)
https://blogs.jpcert.or.jp/ja/2019/04/csirt-1.html

４．海外の動き

● 米国 DHS
・Mozilla が Thunderbird についてのセキュリティアップデートをリリース。(03/25)
https://www.us-cert.gov/ncas/current-activity/2019/03/25/Mozilla-Releases-Security-Update-Thunderbird

・Apple 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。(03/25)
https://www.us-cert.gov/ncas/current-activity/2019/03/25/Apple-Releases-Multiple-Security-Updates

・ASUS 社が Live Update Software についてのセキュリティアップデートをリリース。(03/26)
https://www.us-cert.gov/ncas/current-activity/2019/03/26/ASUS-Releases-Security-Update-Live-Update-Software

・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。(03/27)
https://www.us-cert.gov/ncas/current-activity/2019/03/27/Cisco-Releases-Security-Advisories-Multiple-Products

・Cisco 社が Cisco IOS XE についてのセキュリティアップデートをリリース。(03/28)
https://www.us-cert.gov/ncas/current-activity/2019/03/28/Cisco-Releases-Security-Update-Cisco-IOS-XE

・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。(03/29)
https://www.us-cert.gov/ncas/current-activity/2019/03/29/VMware-Releases-Security-Updates

・４月は全米サプライチェーン保全月間。米国国土安全保障省（ＤＨＳ）サイバーセキュリティ・インフラセキュリティ庁（ＣＩＳＡ）が国家情報長官室による助言を紹介。(04/01)
https://www.us-cert.gov/ncas/current-activity/2019/04/01/Supply-Chain-Integrity-Month

・米国全州情報共有・分析センター（MS-ISAC)がマルウェア「LockerGoga」についてのセキュリティ入門書を公開。(04/01)
https://www.us-cert.gov/ncas/current-activity/2019/04/01/MS-ISAC-Releases-Security-Primer-LockerGoga-Ransomware

・Apache ソフトウェア財団が Apache HTTP Server についてのセキュリティアップデートをリリース。(04/04)
https://www.us-cert.gov/ncas/current-activity/2019/04/04/Apache-Releases-Security-Update-Apache-HTTP-Server

・Samba がセキュリティアップデートをリリース。(04/08)
https://www.us-cert.gov/ncas/current-activity/2019/04/08/Samba-Releases-Security-Updates

・３月２５日の週の脆弱性概報(04/01)
https://www.us-cert.gov/ncas/bulletins/SB19-091

・４月１日の週の脆弱性概報(04/08)
https://www.us-cert.gov/ncas/bulletins/SB19-098

・ENTTEC 社のネットワーク機器に重要な機能に対する認証の欠如の脆弱性。(03/26)
https://ics-cert.us-cert.gov/advisories/ICSA-19-085-03-0
※CVSSv3 では基本値「7.5」となっています。

・Phoenix Contact 社のアクセスポイントにコマンドインジェクションの脆弱性。(03/26)
https://ics-cert.us-cert.gov/advisories/ICSA-19-085-02
※CVSSv3 では基本値「9.9」となっています。

・Siemens 社のイーサネットスイッチに期待される行動の違反の脆弱性。(03/26)
https://ics-cert.us-cert.gov/advisories/ICSA-19-085-01

・Rockwell Automation 社のＡＣドライブに適切でないリソース消費制限の脆弱性。(03/28)
https://ics-cert.us-cert.gov/advisories/ICSA-19-087-01
※CVSSv3 では基本値「7.5」となっています。

・Advantech 社の制御監視システムに不適切なアクセス制御等の脆弱性。(04/02)
https://ics-cert.us-cert.gov/advisories/ICSA-19-092-01
※CVSSv3 では基本値「9.8」となっています。

・Rockwell Automation 社のネットワークセキュリティ機器に不適切な入力検証等の脆弱性。(04/04)
https://ics-cert.us-cert.gov/advisories/ICSA-19-094-04
※CVSSv3 では基本値「8.6」となっています。
https://ics-cert.us-cert.gov/advisories/ICSA-19-094-03
※CVSSv3 では基本値「8.6」となっています。
https://ics-cert.us-cert.gov/advisories/ICSA-19-094-02

・Omron 社のＦＡ用ソフトウェアにメモリの解放後使用の脆弱性。(04/04)
https://ics-cert.us-cert.gov/advisories/ICSA-19-094-01

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、４月２３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