■―――――――――――――――――――――――――――――――――――□

┃　　◆◆　NISC 重要インフラニュースレター　◆◆

┃　　（２０１９年２月２６日発行 第２３２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２３２号の目次　◆―――――――――――――――――――――――┐

├―――――――――――――――――――――――――――――――――――┤

○今号は、２月１３日～２月２５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(APSB19-07)(CVE-2019-7020 等)(IPA、JPCERT/CC)(02/13)

https://www.ipa.go.jp/security/ciadr/vul/20190213-adobereader.html

https://www.jpcert.or.jp/at/2019/at190004.html

・Adobe Flash Player の脆弱性対策について(APSB19-06)(CVE-2019-7090)(IPA、JPCERT/CC)(02/13)

https://www.ipa.go.jp/security/ciadr/vul/20190213-adobeflashplayer.html

https://www.jpcert.or.jp/at/2019/at190005.html

・Adobe Acrobat および Reader の脆弱性対策について(APSB19-13)(CVE-2019-7815)(IPA、JPCERT/CC)(02/22)
https://www.ipa.go.jp/security/ciadr/vul/20190222-adobereader.html
https://www.jpcert.or.jp/at/2019/at190008.html

・Creative Cloud Desktop Application のインストーラにおける DLL 読み込みに関する脆弱性(JVN)(02/19)
https://jvn.jp/jp/JVN50810870/index.html
※CVSSv3 では基本値「7.8」となっています。

（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 2 月) (IPA、JPCERT/CC)(02/13)
https://www.ipa.go.jp/security/ciadr/vul/20190213-ms.html
https://www.jpcert.or.jp/at/2019/at190006.html

（３）Intel 社製品に関する脆弱性
・Intel 製品に複数の脆弱性(JVN)(02/13)
https://jvn.jp/vu/JVNVU99119322/index.html

（４）その他
・runc の権限昇格の脆弱性（CVE-2019-5736）に関する注意喚起(JPCERT/CC)(02/14)
https://www.jpcert.or.jp/at/2019/at190007.html

・ISC BIND 9 に複数の脆弱性(JPCERT/CC、JVN)(02/22)
https://www.jpcert.or.jp/at/2019/at190009.html
https://jvn.jp/vu/JVNVU92881878/index.html
※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
・約束のネバーランド×サイバーセキュリティ月間　特別イベント「抗え。この世界（インターネット）の脅威に。」の開催を決定(02/15)
https://www.nisc.go.jp/security-site/files/event_2019.pdf

（２）総務省
・サイバーセキュリティ人材育成分科会（第 3 回）(02/12)

http://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00019.html

・「サイバーセキュリティに関する総務大臣奨励賞」の受賞者の公表(02/21)
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00017.html

■―――――――――――――――――――――――――――――――――□

┃３．関係機関の動き

┼―――――――――――――――――――――――――――――――――┼

（１）ＩＰＡ

・プレス発表　ツールを用いた効率的なソフトウェアの脆弱性対策を解説した資料を公開(02/21)
https://www.ipa.go.jp/about/press/20190221.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・CyberNewsFlash「複数の Adobe 製品のアップデートについて」を公開(02/13)
https://www.jpcert.or.jp/newsflash/2019021301.html

・CyberNewsFlash「QNAP 社製 NAS に影響を与えるマルウエアに関する情報について」を公開(02/15)
https://www.jpcert.or.jp/newsflash/2019021501.html

・JPCERT/CC Eyes「攻撃グループ Tick による日本の組織をターゲットにした攻撃活動」(02/19)
https://blogs.jpcert.or.jp/ja/2019/02/tick-activity.html

・Weekly Report 2019-02-20 号(02/20)
https://www.jpcert.or.jp/wr/2019/wr190701.html

□―――――――――――――――――――――――――――――――――■

┃４．海外の動き

┼―――――――――――――――――――――――――――――――――┼

（１）US-CERT

・Cisco 社が Network Assurance Engine についてのセキュリティアップデートをリリース。(02/12)
https://www.us-cert.gov/ncas/current-activity/2019/02/12/Cisco-Releases-Security-Update

・米国連邦取引委員会（ＦＴＣ）がインターネットロマンス詐欺に関する報告を公開。(02/12)
https://www.us-cert.gov/ncas/current-activity/2019/02/12/Internet-Romance-Scams

・Mozilla が Firefox 及び Firefox ESR についてのセキュリティアップデートをリリース。(02/12)
https://www.us-cert.gov/ncas/current-activity/2019/02/12/Mozilla-Releases-Security-Updates-Firefox

・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。(02/14)
https://www.us-cert.gov/ncas/current-activity/2019/02/14/Mozilla-Releases-Security-Update-Thunderbird

・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。(02/15)
https://www.us-cert.gov/ncas/current-activity/2019/02/15/VMware-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。(02/20)
https://www.us-cert.gov/ncas/current-activity/2019/02/20/Cisco-Releases-Security-Updates

・Drupal が Drupal Core についてのセキュリティアップデートをリリース。(02/21)
https://www.us-cert.gov/ncas/current-activity/2019/02/21/Drupal-Releases-Security-Updates

・２月１８日の週の脆弱性概報(02/25)
https://www.us-cert.gov/ncas/bulletins/SB19-056

（２）米 ICS-CERT
・Siemens 社のオートメーションシステムにクロスサイトスクリプティング等の脆弱性(02/12)
https://ics-cert.us-cert.gov/advisories/ICSA-19-043-06
※CVSSv3 では基本値「9.1」となっています。

・Siemens 社のオートメーションシステムにリソース管理エラー等の脆弱性(02/12)
https://ics-cert.us-cert.gov/advisories/ICSA-19-043-05

・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(02/12)
https://ics-cert.us-cert.gov/advisories/ICSA-19-043-04
※CVSSv3 では基本値「7.5」となっています。

・Siemens 社の暗号化ツールにヒープベースのバッファオーバーフロー等の脆弱性(02/12)
https://ics-cert.us-cert.gov/advisories/ICSA-19-043-03
※CVSSv3 では基本値「10.0」となっています。

・Siemens 社のイーサネット通信モジュールに不適切な入力検証の脆弱性(02/12)
https://ics-cert.us-cert.gov/advisories/ICSA-19-043-02

※CVSSv3 では基本値「7.5」となっています。

・OSIsoft 社の画像化ツールにクロスサイトスクリプティングの脆弱性(02/12)
https://ics-cert.us-cert.gov/advisories/ICSA-19-043-01

・gpsd Open Source Project のＧＰＳデータ変換ソフト等にスタックベースのバッファオーバーフローの脆弱性(02/14)
https://ics-cert.us-cert.gov/advisories/ICSA-18-310-01
※CVSSv3 では基本値「8.3」となっています。

・Pangea Communications 社のＦＡＸ　ＡＴＡに代替経路やチャネルによる認証機構の迂回の脆弱性(02/14)
https://ics-cert.us-cert.gov/advisories/ICSA-19-045-01
※CVSSv3 では基本値「7.5」となっています。

・Rockwell Automation 社の電力モニターにクロスサイトスクリプティング等の脆弱性(02/19)
https://ics-cert.us-cert.gov/advisories/ICSA-19-050-04
※CVSSv3 では基本値「9.8」となっています。

・Horner Automation 社のＰＬＣソフトに不適切な入力検証の脆弱性(02/19)
https://ics-cert.us-cert.gov/advisories/ICSA-19-050-03
※CVSSv3 では基本値「7.8」となっています。

・Delta Electronics 社の産業用オートメーションソフトに領域外のメモリ参照の脆弱性(02/19)
https://ics-cert.us-cert.gov/advisories/ICSA-19-050-02

・Intel 社のデータセンター管理ソフトに不適切な認証等の脆弱性(02/19)
https://ics-cert.us-cert.gov/advisories/ICSA-19-050-01
※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、３月１２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――――┤

■――□