■―――――――――――――――――――――――――――――――――□

┃　　◆◆　NISC 重要インフラニュースレター　◆◆

┃　　（２０１９年５月１４日発行 第２３７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２３７号の目次　◆―――――――――――――――――――――┐

├―――――――――――――――――――――――――――――――――┤

○今号は、４月２３日～５月１３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）Oracle 社製品に関する脆弱性

・Oracle WebLogic Server の脆弱性（CVE-2019-2725）について(IPA、JPCERT/CC)(04/28)

https://www.ipa.go.jp/security/ciadr/vul/20190428_WebLogicServer.html

https://www.jpcert.or.jp/at/2019/at190020.html

※CVSSv3 では基本値「9.8」となっています。

（２）その他

・ISC BIND 9 に対する複数の脆弱性に関する注意喚起(JPCERT/CC、JVN)(04/25)

https://www.jpcert.or.jp/at/2019/at190019.html

https://jvn.jp/vu/JVNVU99876126/index.html

※CVSSv3 では基本値「7.5」となっています。

・サイボウズ Garoon における複数の脆弱性(JVN)(04/25)
https://jvn.jp/jp/JVN58849431/index.html
※CVSSv3 では基本値「7.4」となっています。

・PrinterLogic 製 Print Management software における SSL 証明書やソフトウェアアップデートの整合性の検証をしない脆弱性(JVN)(05/07)
https://jvn.jp/vu/JVNVU90648875/index.html

・Android アプリ「クリエイトＳＤ公式アプリ」におけるアクセス制限不備の脆弱性(JVN)(05/10)
https://jvn.jp/jp/JVN87655507/index.html

・電子申請・届出アプリケーション オンライン版のインストーラにおける DLL 読み込みに関する脆弱性(JVN)(05/10)
https://jvn.jp/jp/JVN91361851/index.html
※CVSSv3 では基本値「7.8」となっています。

・電子申請・届出アプリケーション オフライン版における DLL 読み込みに関する脆弱性(JVN)(05/10)
https://jvn.jp/jp/JVN69903953/index.html
※CVSSv3 では基本値「7.8」となっています。

２．政府機関の動き

（１）ＮＩＳＣ
・ 重要インフラ専門調査会第 18 回会合を開催（4/18 開催）(04/26)
https://www.nisc.go.jp/conference/cs/ciip/index.html#ciip18

（２）総務省
・サイバーセキュリティ人材育成分科会（第 5 回）(04/25)

http://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00036.html

・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(05/10)
http://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00039.html

３．関係機関の動き

（１）ＩＰＡ

・「情報セキュリティ安心相談窓口の相談状況［2019 年第 1 四半期（1 月～3 月）］」を公開しました。(04/23)

https://www.ipa.go.jp/security/txt/2019/q1outline.html

・脆弱性対策情報データベース JVN iPedia の登録状況［2019 年第 1 四半期（1 月～3 月）］(04/24)

https://www.ipa.go.jp/security/vuln/report/JVNiPedia2019q1.html

・「サイバー情報共有イニシアティブ（J-CSIP） 運用状況［2019 年 1 月～3 月]」を公開しました。（04/25)

https://www.ipa.go.jp/security/J-CSIP/index.html

・ソフトウェア等の脆弱性関連情報に関する届出状況[2019 年第 1 四半期（1 月～3 月）](IPA、JPCERT/CC)(04/25)

https://www.ipa.go.jp/security/vuln/report/vuln2019q1.html

https://www.jpcert.or.jp/report/press.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2019-04-24 号(04/24)

https://www.jpcert.or.jp/wr/2019/wr191601.html

・Weekly Report 2019-05-09 号(05/09)

https://www.jpcert.or.jp/wr/2019/wr191701.html

４．海外の動き

● 米国 DHS

・オランダサイバーセキュリティセンター（ＮＣＳＣ）が、ＴＬＳガイドラインの改定版を公表。(04/23)

https://www.us-cert.gov/ncas/current-activity/2019/04/23/Dutch-NCSC-Releases-Updated-TLS-Guidelines

・米国連邦取引委員会（ＦＴＣ）が親が子供のインターネット上の安全を確保するヒント集を公開。(04/26)

https://www.us-cert.gov/ncas/current-activity/2019/04/26/FTC-Releases-Article-Keeping-Children-Safe-Online

・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）が脆弱性対策に関する指令を公表。(04/30)
https://www.us-cert.gov/ncas/current-activity/2019/04/30/CISA-Releases-Binding-Operational-Directive-Vulnerability

・Google が Windows、Mac 及び Linux 向けの Chrome version 74.0.3729.131 をリリース。(04/30)
https://www.us-cert.gov/ncas/current-activity/2019/04/30/Google-Releases-Security-Updates-Chrome

・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。(05/01)
https://www.us-cert.gov/ncas/current-activity/2019/05/01/Cisco-Releases-Security-Updates
https://www.us-cert.gov/ncas/current-activity/2019/05/07/Cisco-Releases-Security-Update-Elastic-Services-Controller
https://www.us-cert.gov/ncas/current-activity/2019/05/13/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。(05/09)
https://www.us-cert.gov/ncas/current-activity/2019/05/09/Drupal-Releases-Security-Update

・安全性が確保されていないＳＡＰ社システムの新たな悪用。(05/02)
https://www.us-cert.gov/ncas/alerts/AA19-122A

・マルウェア分析レポート：北朝鮮政府によるトンネリングツール「ELECTRICFISH」(05/09)
https://www.us-cert.gov/ncas/analysis-reports/AR19-129A

・分析レポート：Microsoft Office 365 に係るセキュリティ監視(05/13)
https://www.us-cert.gov/ncas/analysis-reports/AR19-133A

・４月２２日の週の脆弱性概報(04/29)
https://www.us-cert.gov/ncas/bulletins/SB19-119

・４月２９日の週の脆弱性概報(05/06)
https://www.us-cert.gov/ncas/bulletins/SB19-126

・５月６日の週の脆弱性概報(05/13)
https://www.us-cert.gov/ncas/bulletins/SB19-133

・富士フィルム社の画像診断システムに不適切なアクセス制御等の脆弱性。(04/23)

https://ics-cert.us-cert.gov/advisories/ICSMA-19-113-01
※CVSSv3 では基本値「9.8」となっています。

・Rockwell Automation 社のプログラマブルコントローラにスタックベースのバッファオーバーフロー等の脆弱性。(04/30)
https://ics-cert.us-cert.gov/advisories/ICSA-19-120-01
※CVSSv3 では基本値「8.6」となっています。

・Philips 社の電子カルテシステムにクロスサイトスクリプティングの脆弱性。(04/30)
https://ics-cert.us-cert.gov/advisories/ICSMA-19-120-01

・Sierra Wireless 社のルーターに情報漏洩等の脆弱性。(05/02)
https://ics-cert.us-cert.gov/advisories/ICSA-19-122-03
※CVSSv3 では基本値「9.1」となっています。

・ＧＥ社の電力計に不適切なアクセス制御等の脆弱性。(05/02)
https://ics-cert.us-cert.gov/advisories/ICSA-19-122-02
※CVSSv3 では基本値「8.1」となっています。

・Orpak 社の燃料充填自動化ソフト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。(05/02)
https://ics-cert.us-cert.gov/advisories/ICSA-19-122-01
※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、５月２８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────┤

■──□