BEZPEČNOSTNÝ BULLETIN

Týždeň 19. 06. 2019 - 25. 06. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01380/2019/TS/OKB-169

BEZPEČNOSTNÝ BULLETIN

Týždeň 19. 06. 2019 - 25. 06. 2019

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dell SupportAssist zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt SupportAssist, ktorá opravuje bezpečnostnú zraniteľnosť v komponente PC Doctor.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

21.06.2019

CVE

CVE-2019-12280

Zasiahnuté systémy

Dell SupportAssist for Business PCs verzie staršie ako 2.0.1
Dell SupportAssist for Home PCs verzie staršie ako 3.2.2

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.dell.com/support/article/sk/sk/skdhs1/sln317291/dsa-2019-084-dell-supportassist-for-business-pcs-and-dell-supportassist-for-home-pcs-security-update-for-pc-doctor-vulnerability
https://www.helpnetsecurity.com/2019/06/21/dell-supportassist-cve-2019-12280/
https://www.techradar.com/news/major-security-flaw-hits-dell-pcs-and-potentially-millions-of-other-laptops

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01380/2019/TS/OKB-169

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PostgreSQL zraniteľnosť

Popis

Vývojári databázového systému PostgreSQL vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.06.2019

CVE

CVE-2019-10164

Zasiahnuté systémy

PostgreSQL verzie staršie ako 9.4.23
PostgreSQL verzie staršie ako 9.5.18
PostgreSQL verzie staršie ako 9.6.14
PostgreSQL verzie staršie ako 10.9.0
PostgreSQL verzie staršie ako 11.4.0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.postgresql.org/about/news/1949/
https://tools.cisco.com/security/center/viewAlert.x?alertId=60379

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PHOENIX CONTACT Automation Worx zraniteľnosti

Popis

Bezpečnostní výskumníci informovali o zraniteľnostiach v produkte Phoenix Contact Automation Worx. Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.06.2019

CVE

CVE-2019-12869, CVE-2019-12870, CVE-2019-12871

Zasiahnuté systémy

Phoenix Contact Automation Worx Software Suite verzia 1.86

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Na uvedené zraniteľnosti spoločnosť Phoenix Contact doposiaľ nevydala bezpečnostné aktualizácie. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-171-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Sony VAIO Update zraniteľnosti

Popis

Spoločnosť Sony vydala bezpečnostnú aktualizáciu na svoj produkt VAIO Update, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosť sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.06.2019

CVE

CVE-2019-5981, CVE-2019-5982

Zasiahnuté systémy

Sony VAIO Update verzie staršie ako 7.4.0.15200

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.sony.com/electronics/support/articles/00228777
http://jvn.jp/en/jp/JVN13555032/index.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/162810
https://exchange.xforce.ibmcloud.com/vulnerabilities/162809

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zero-Day zraniteľnosť Mozilla Firefox

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje produkty Firefox a Firefox ESR, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov získať neoprávnený prístup do systému.
Uvedená zraniteľnosť je v súčasnosti aktívne využívaná útočníkmi.

Dátum prvého zverejnenia varovania

20.06.2019

CVE

CVE-2019-11708

Zasiahnuté systémy

Firefox verzie staršie ako 67.0.4
Firefox ESR verzie staršie ako 60.7.2

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov a následne vykonať ich kontrolu prostriedkami antivírusovej a antimalwarovej kontroly. V prípade pozitívneho nálezu rovnako odporúčame vykonať zmenu všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2019-19/
https://access.redhat.com/security/cve/cve-2019-11708
https://thehackernews.com/2019/06/firefox-0day-vulnerability.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux kernel a FreeBSD Kernel zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostných zraniteľnostiach v produktoch Linux Kernel a FreeBSD Kernel.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených TCP paketov spôsobiť zneprístupnenie služby.
Na uvedenú zraniteľnosť je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

17.06.2019

CVE

CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-5599

Zasiahnuté systémy

Linux Kernel verzie staršie ako 4.15 a 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11
FreeBSD 12

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade, že aktualizácia nie je možná, odporúčame zabezpečiť systém podľa návodu zverejnenom na: https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md

Zdroje

https://www.tenable.com/blog/sack-panic-linux-and-freebsd-kernels-vulnerable-to-remote-denial-of-service-vulnerabilities-cve
https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md
https://access.redhat.com/security/cve/cve-2019-11477
https://access.redhat.com/security/cve/cve-2019-11478
https://access.redhat.com/security/cve/cve-2019-11479

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Tomcat zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie na svoj produkt Tomcat, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.06.2019

CVE

CVE-2019-10072

Zasiahnuté systémy

Apache Tomcat verzie staršie ako 9.0.20
Apache Tomcat verzie staršie ako 8.5.41

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://tomcat.apache.org/security-8.html
http://tomcat.apache.org/security-9.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=60390

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť Outlook pre Android

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj produkt Outlook pre Android, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej URL adresy získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.06.2019

CVE

CVE-2019-1105

Zasiahnuté systémy

Outlook pre Android verzie staršie ako 3.0.88

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1105
https://www.f5.com/labs/articles/threat-intelligence/how-i-hacked-the-microsoft-outlook-android-app-and-found-cve-2019-1105
https://thehackernews.com/2019/06/outlook-app-android.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Pydio Cells zraniteľnosti

Popis

Spoločnosť Pydio vydala bezpečnostnú aktualizáciu na svoj produkt Cells, ktoré opravujú bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej URL adresy vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

20.06.2019

CVE

CVE-2019-12901, CVE-2019-12902, CVE-2019-12903

Zasiahnuté systémy

Pydio Cells verzie staršie ako 1.5.0

Následky

Neoprávnená zmena v systéme
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://research.loginsoft.com/vulnerability/multiple-vulnerabilities-in-pydio-cells-1-4-1/
https://exchange.xforce.ibmcloud.com/vulnerabilities/162819
https://exchange.xforce.ibmcloud.com/vulnerabilities/162820
https://exchange.xforce.ibmcloud.com/vulnerabilities/162827

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01380/2019/TS/OKB-169