BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 12. 2020 - 08. 12. 2020

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:
01439/2020/SK-CERT-277

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v Xerox DocuShare

Popis

Spoločnosť Xerox vydala bezpečnostnú aktualizáciu pre svoj produkt na zdieľanie dokumentov DocuShare, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného XML súboru vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.11.2020

CVE

CVE-2020-27177

Zasiahnuté systémy

Xerox DocuShare verzie staršie ako 6.61 Update 3 Patch 4 Hotfix 9
Xerox DocuShare verzie staršie ako 7.0 Update 1 Patch 3 Hotfix 22
Xerox DocuShare verzie staršie ako 7.5 Hotfix 2

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom 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 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://securitydocs.business.xerox.com/wp-content/uploads/2020/11/cert_Security_Mini_Bulletin_XRX20W_for-DocuShare-6.61_7.0_7.5.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Viacero zraniteľností v Google Chrome

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu pre svoj internetový prehliadač Chrome, ktorá opravuje viacero zraniteľností.
Najzávažnejšia zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvoreného súboru vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.12.2020

CVE

CVE-2020-16037, CVE-2020-16038, CVE-2020-16039, CVE-2020-16040, CVE-2020-16041, CVE-2020-16042

Zasiahnuté systémy

Google Chrome verzie staršie ako 87.0.4280.88

Následky

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

Odporúčania

Administrátorom a používateľom 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 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://chromereleases.googleblog.com/2020/12/stable-channel-update-for-desktop.html
https://its.ny.gov/security-advisory/multiple-vulnerabilities-197
https://www.securitylab.ru/vulnerability/514570.php

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosti v RedHat Enterprise Linuxe

Popis

Spoločnosť Red Hat vydala bezpečnostné aktualizácie na svoj operačný systém Red Hat Enterprise Linux, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť, nachádzajúca sa v knižnici PostgreSQL, spočíva v nedostatočnej imlementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom vytvorenia špeciálne vytvoreného súboru vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.12.2020

CVE

CVE-2019-14868, CVE-2020-14385, CVE-2020-14386, CVE-2020-15862, CVE-2020-16012, CVE-2020-25638, CVE-2020-25644, CVE-2020-25649, CVE-2020-25694, CVE-2020-25695, CVE-2020-25696, CVE-2020-26950, CVE-2020-26951, CVE-2020-26953, CVE-2020-26956, CVE-2020-26958, CVE-2020-26959, CVE-2020-26960, CVE-2020-26961, CVE-2020-26965, CVE-2020-26968

Zasiahnuté systémy

ksh 93 pre Red Hat Enterprise Linux 7.3
net-snmp pre Red Hat Enterprise Linux 7
Red Hat JBoss Enterprise Application Platform verzie staršie ako 7.3.4
rh-postgresql12-postgresql pre Red Hat Software Collections verzie staršie ako 12.5
rh-postgresql12-postgresql pre Red Hat Software Collections verzie staršie ako 10.15
Mozilla Firefox pre Red Hat Enterprise Linux 8.0 verzie staršie ako 78.5.0
Mozilla Thunderbird pre Red Hat Enterprise Linux 8.0 verzie staršie ako 78.4.3

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom
Eskalácia privilégií

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://access.redhat.com/errata/RHSA-2020:5167
https://access.redhat.com/errata/RHSA-2020:5199
https://access.redhat.com/errata/RHSA-2020:5351
https://access.redhat.com/errata/RHSA-2020:5352
https://access.redhat.com/errata/RHSA-2020:5350
https://access.redhat.com/errata/RHSA-2020:5344
https://access.redhat.com/errata/RHSA-2020:5342
https://access.redhat.com/errata/RHSA-2020:5341
https://access.redhat.com/errata/RHSA-2020:5340
https://access.redhat.com/errata/RHSA-2020:5317
https://access.redhat.com/errata/RHSA-2020:5316
https://access.redhat.com/errata/RHSA-2020:5314

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

Identifikátor

Viacero zraniteľností Apple iCloud pre Windows

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností produktu iCloud.
Najzávažnejšia zraniteľnosť umožňuje lokálnemu autentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvoreného súboru vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.12.2020

CVE

CVE-2020-10002, CVE-2020-13434, CVE-2020-13435, CVE-2020-13630, CVE-2020-13631, CVE-2020-27911, CVE-2020-27912, CVE-2020-27917, CVE-2020-27918, CVE-2020-9849, CVE-2020-9876, CVE-2020-9947, CVE-2020-9951, CVE-2020-9961, CVE-2020-9981, CVE-2020-9983

Zasiahnuté systémy

Apple iCloud pre Windows verzie staršie ako 11.5

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom 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://support.apple.com/sk-sk/HT211935

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

Identifikátor

Zraniteľnosť v Mozilla Thunderbird

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu pre svoj produkt Mozilla Thunderbird, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej požiadavky vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.12.2020

CVE

CVE-2020-26970

Zasiahnuté systémy

Mozilla Thunderbird verzie staršie ako 78.5.1

Následky

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

Odporúčania

Administrátorom a používateľom 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 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.mozilla.org/en-US/security/advisories/mfsa2020-53/
https://cert.pse-online.pl/mozilla-publikuje-aktualizacje-zabezpieczen-dla-produktu-thunderbird/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v Schneider Electric EcoStruxure Operator Terminal Expert

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu pre svoj softvér pre správu industriálnych systémov, ktorá upravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, neautentifikovanému útočníkovi vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.12.2020

CVE

CVE-2020-7544

Zasiahnuté systémy

Schneider Electric EcoStruxure Operator Terminal Expert runtime verzie staršie ako 3.1 Service Pack 1B

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Po odstránení zraniteľnosti, 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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-336-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť vo viacerých produktoch VMware

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť vo viacerých produktoch.
Zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému, antentifikovanému útočníkovi s administrátorskými právami vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

03.12.2020

CVE

CVE-2020-4006

Zasiahnuté systémy

VMware Workspace ONE Access verzie staršie ako 20.10 pre Linux
VMware Workspace ONE Access verzie staršie ako 20.01 pre Linux
VMware Identity Manager verzie staršie ako 3.3.3 pre Linux
VMware Identity Manager verzie staršie ako 3.3.2 pre Linux
VMware Identity Manager verzie staršie ako 3.3.1 pre Linux
VMware Identity Manager Connector verzie staršie ako 3.3.2, 3.3.1 pre Linux
VMware Identity Manager Connector verzie staršie ako 3.3.3, 3.3.2, 3.3.1 pre Windows
VMware Identity Manager Connector verzie staršie ako 19.03 pre Windows
VMware Identity Manager Connector verzie staršie ako 19.03.0.1 pre Windows

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľnosti, 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.vmware.com/security/advisories/VMSA-2020-0027.html
https://kb.vmware.com/s/article/81754

Dôležitosť	☐ Nízka	☒ Stredná	☐ Vysoká	☐ Kritická	CVSS skóre: 5.4
Klasifikácia	☒ Neutajované / TLP(WHITE)		☐ Vyhradené	☐ Dôverné	☐ Tajné
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v Apache Tomcat

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Tomcat, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

03.12.2020

CVE

CVE-2020-17527

Zasiahnuté systémy

Apache Tomcat verzie od 10.0.0-M1 a staršie ako 10.0.0-M10
Apache Tomcat verzie od 9.0.0.M5 a staršie ako 9.0.40
Apache Tomcat verzie od 8.5.1 a staršie ako 8.5.60

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

http://mail-archives.us.apache.org/mod_mbox/www-announce/202012.mbox/<52858194-2efd-6f17-1821-9036c8494df0%40apache.org>