BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 09. 2019 - 24. 09. 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-228

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

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie z týchto zraniteľností sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.09.2019

CVE

CVE-2019-13685, CVE-2019-13686, CVE-2019-13687, CVE-2019-13688

Zasiahnuté systémy

Google Chrome verzie staršie ako 77.0.3865.90

Následky

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

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 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/2019/09/stable-channel-update-for-desktop_18.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-095/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Micro Focus Data Protector zraniteľnosť

Popis

Spoločnosť Micro Focus vydala bezpečnostnú aktualizáciu na svoj produkt Data Protector, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

13.09.2019

CVE

CVE-2019-11660

Zasiahnuté systémy

Micro Focus Data Protector verzie staršie ako 2019.08 (A.10.50)

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03525630

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

RSA Archer viacero zraniteľností

Popis

Spoločnosť RSA vydala bezpečnostnú aktualizáciu na svoj produkt Archer, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

28.08.2019

CVE

CVE-2019-3756, CVE-2019-3758

Zasiahnuté systémy

RSA Archer verzie staršie ako 6.6 P3 (6.6.0.3), 6.5 P6 (6.5.0.6) a 6.4. SP1 P7 (6.4.1.7)

Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://community.rsa.com/docs/DOC-106759
https://www.dell.com/support/security/sk-sk/details/DOC-106759/DSA-2019-127-RSA-Archer-Security-Update-for-Multiple-Vulnerabilities#

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens SINEMA Remote Connect Server viacero zraniteľností

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoj produkt SINEMA Remote Connect Server, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť vo webovom rozhraní je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.09.2019

CVE

CVE-2019-13918, CVE-2019-13919, CVE-2019-13920, CVE-2019-13922

Zasiahnuté systémy

Siemens SINEMA Remote Connect Server verzie staršie ako V2.0 SP1

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-884497.pdf
https://www.us-cert.gov/ics/advisories/icsa-19-260-02

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

Identifikátor

Tridium Niagara zraniteľnosti

Popis

Spoločnosť Tridium vydala bezpečnostnú aktualizáciu na svoj produkt Niagara, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

27.08.2019

CVE

CVE-2019-13528, CVE-2019-8998

Zasiahnuté systémy

Niagara AX 3.8u4 verzie staršie ako OS Dist: 2.7.402.2NRE Config Dist: 3.8.401.1
Niagara 4.4u3 verzie staršie ako OS Dist: 4.4.73.38.1 NRE Config Dist: 4.4.94.14.1
Niagara 4.7u1 verzie staršie ako OS Dist: (JACE 8000) 4.7.109.16.1OS Dist (Edge 10): 4.7.109.18.1 NRE Config Dist: 4.7.110.32.1

Následky

Eskalácia privilégií
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.tridium.com/~/media/tridium/library/documents/collateral/technical%20bulletins/qnx_vulnerability_fix.ashx?la=en
http://support.blackberry.com/kb/articleDetail?articleNumber=000057178
https://www.us-cert.gov/ics/advisories/icsa-19-262-01

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

Identifikátor

Zraniteľnosti Microsoft produktov

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v skriptovacom engine internetového prehliadača Internet Explorer a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Uvedená zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

23.09.2019

CVE

CVE-2019-1255, CVE-2019-1367

Zasiahnuté systémy

Internet Explorer 9, 10, 11
Microsoft Forefront Endpoint Protection 2010
Microsoft Security Essentials
Microsoft System Center 2012 Endpoint Protection
Microsoft System Center 2012 R2 Endpoint Protection
Microsoft System Center Endpoint Protection
Windows Defender

Následky

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

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 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://exchange.xforce.ibmcloud.com/vulnerabilities/167366 https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-internet-explorer-and-microsoft-defender-could-allow-for-arbitrary-code-execution_2019-096/ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1255 https://www.zdnet.com/article/microsoft-releases-out-of-band-security-update-to-fix-ie-zero-day-defender-bug/

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

Identifikátor

Atlassian Jira viacero zraniteľností

Popis

Spoločnosť Atlassian vydala bezpečnostné aktualizácie na svoje produkty Jira Service Desk, Server a Data Center, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

18.09.2019

CVE

CVE-2019-14994, CVE-2019-15001

Zasiahnuté systémy

Jira Server & Jira Data Center verzie staršie ako 7.6.16, 7.13.8, 8.1.3, 8.2.5, 8.3.4, 8.4.1
Jira Service Desk verzie staršie ako 3.9.16, 3.16.8, 4.1.3, 4.2.5, 4.3.4, 4.4.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme

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://confluence.atlassian.com/jira/jira-security-advisory-2019-09-18-976766250.html
https://confluence.atlassian.com/jira/jira-service-desk-security-advisory-2019-09-18-976171274.html
https://www.bleepingcomputer.com/news/security/jira-server-and-service-desk-fix-critical-security-bugs/
https://www.tenable.com/blog/cve-2019-14994-url-path-traversal-vulnerability-in-jira-service-desk-leads-to-information

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

Identifikátor

Micro Focus Service Manager zraniteľnosti

Popis

Spoločnosť Micro Focus vydala bezpečnostnú aktualizáciu na svoj produkt Service Manager, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

09.09.2019

CVE

CVE-2018-0732, CVE-2018-0737, CVE-2019-11661, CVE-2019-11662, CVE-2019-11663, CVE-2019-11664, CVE-2019-11665, CVE-2019-11666

Zasiahnuté systémy

Micro Focus Service Manager verzie staršie ako 9.63 a 9.35 P7

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme
Zneprístupnenie služby

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://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03518316