BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 02. 2018 – 20. 02. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Číslo	Identifikátor	Dôležitosť	CVSS Skóre
1	Chrome Stable Channel Update for Desktop	Vysoká	8.8
2	IBM Notes and Client Application Access Privilege Escalation vulnerabilities	Vysoká	8.4
3	SAP Security Patch	Vysoká	8.3
4	Xen Hypervisor Multiple Vulnerabilities	Vysoká	7.8
5	NetBSD Multiple Vulnerabilities	Vysoká	7.5
6	Schneider Electric multiple products vulnerabilities	Vysoká	7.2
7	Bugzilla report.cgi Cross-Site Request Forgery Vulnerability	Stredná	6.5

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:
02049/2018/TS/OKB-008

BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 02. 2018 – 20. 02. 2018

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

Identifikátor

Chrome Stable Channel Update for Desktop

Popis

Spoločnosť Google vydala aktualizáciu na produkt Google Chrome, ktorá obsahuje opravu viacerých chýb a bezpečnostnej zraniteľnosti v komponente JavaScript Interpreter (Chrome V8). Vzdialený útočník by zraniteľnosť mohol prostredníctvom podvrhnutého webového obsahu zneužiť na vykonanie škodlivého kódu alebo spôsobiť pád aplikácie.

Dátum prvého zverejnenia varovania

13.02.2018

CVE

CVE-2018-6056

Zasiahnuté systémy

Google Chrome verzie 62.0 (.3202.62, .3202.74, .3202.89, .3202.94); 63.0 (.3239.84, .3239.108, .3239.132) a 64.0 (.3282.119, .3282.140)

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať zasiahnutých produktov.

Zdroje

https://chromereleases.googleblog.com/2018/02/stable-channel-update-for-desktop_13.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM Notes and Client Application Access Privilege Escalation Vulnerabilities

Popis

Spoločnosť IBM vydala aktualizácie na svoje produkty Client Application Access a Notes, ktoré opravujú viacero bezpečnostných zraniteľností. Lokálny útočník by mohol prostredníctvom príkazov zadávaných do zdieľanej pamäte IPC zneužiť systémovú službu Notes System Diagnostic (NSD) na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

16.02.2018

CVE

CVE-2017-1720, CVE-2018-1409, CVE-2018-1410, CVE-2018-1411

Zasiahnuté systémy

IBM Client Application Access verzie 1.0.1
IBM Client Application Access verzie 1.0.1.1
IBM Client Application Access verzie 1.0.1.2
IBM Notes verzie 9.0.1 až 9.0.1 FP10
IBM Notes verzie 9.0 až 9.0 IF4
IBM Notes verzie 8.5.3 až 8.5.3 FP6 IF15
IBM Notes verzie 8.5.2 až 8.5.2 FP4 IF3
IBM Notes verzie 8.5.1. až 8.5.1 FP5 IF3
IBM Notes verzie 8.5

Následky

Vykonanie škodlivého kódu, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg22010766
http://www-01.ibm.com/support/docview.wss?uid=swg22010767

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SAP Security Patch

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Bližšie nešpecifikované bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

13.02.2018

CVE

CVE-2018-2367, CVE-2018-2368, CVE-2018-2372, CVE-2018-2373, CVE-2018-2374, CVE-2018-2375, CVE-2018-2376, CVE-2018-2377, CVE-2018-2378, CVE-2018-2379, CVE-2018-2380, CVE-2018-2381, CVE-2018-2382, CVE-2018-2383, CVE-2018-2384, CVE-2018-2385, CVE-2018-2386, CVE-2018-2387, CVE-2018-2388, CVE-2018-2389, CVE-2018-2390, CVE-2018-2391, CVE-2018-2392, CVE-2018-2393, CVE-2018-2394, CVE-2018-2395, CVE-2018-2396

Zasiahnuté systémy

SAP Internet Graphics Server verzie 7.20, 7.20EXT, 7.45, 7.49, 7.53
SAP Netweaver System Landscape Directory
SAP HANA Extended Application Services
SAP ERP Financials Information System
SAP CRM verzie 7.01, 7.02, 7.30, 7.31, 7.33, 7.54

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://blogs.sap.com/2018/02/13/sap-security-patch-day-february-2018/

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

Identifikátor

Xen Hypervisor Multiple Vulnerabilities

Popis

Produkt Xen Hypervisor obsahuje viacero zraniteľností, ktoré by lokálny útočník mohol zneužiť na zneprístupnenie služieb. Zraniteľnosti spočívajú v nedostatočnej ochrane pred pretečením zásobníka a nesprávnom spracovaní chybových stavov. Lokálny útočník prostredníctvom nich mohol vyvolať pád hypervisora a spôsobiť tak zneprístupnenie poskytovaných služieb. Za špecifických podmienok by útočník mohol vyvolať poškodenie pamäte, ktoré by mu umožnilo eskaláciu privilégií.
Zraniteľnosti ovplyvňujú len Xen bežiaci na x86 systémoch a možno ich zneužiť len z guest systémov bežiacich v režimoch Log-dirty a Shadow.

Dátum prvého zverejnenia varovania

15.02.2018

CVE

CVE-2017-17563, CVE-2017-17564, CVE-2017-17565, CVE-2017-17566

Zasiahnuté systémy

Xen Hypervisor verzie 4.1.0, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5; 4.2.1, 4.2.2, 4.2.3; 4.3.0; 4.4.0, 4.4.1; 4.5.0, 4.5.3; 4.6.0, 4.6.3; 4.7; 4.8; 4.9

Následky

Zneprístupnenie služby, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56841
https://tools.cisco.com/security/center/viewAlert.x?alertId=56842
https://tools.cisco.com/security/center/viewAlert.x?alertId=56843
https://tools.cisco.com/security/center/viewAlert.x?alertId=56844

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

Identifikátor

NetBSD Multiple Vulnerabilities

Popis

Operačný systém NetBSD obsahuje viacero zraniteľností, ktoré by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služieb.
Prvá zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a útočník by prostredníctvom podvrhnutého IPSec IPv6-AH paketu mohol spôsobiť pád jadra.
Druhá zraniteľnosť spočíva v nesprávnom spracovávaní IPv6 paketov a útočník by prostredníctvom špeciálnej sekvencie IPv6 paketov mohol vyvolať chybu pamäte vedúcu k zneprístupneniu služieb.

Dátum prvého zverejnenia varovania

19.02.2018

CVE

-

Zasiahnuté systémy

NetBSD verzie 6.0 (.0, .1, .2, .3, .4, .5); 6.1 (.0, .1, .2, .3, .4); 7.0 (.0, .1, .2); 7.1 (.0)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56860
http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2018-003.txt.asc
https://tools.cisco.com/security/center/viewAlert.x?alertId=56861
http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2018-004.txt.asc

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

Identifikátor

Schneider Electric Multiple Products Vulnerabilities

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na svoje produkty IGSS SCADA, IGSS Mobile a StruxureOn Gateway, ktoré opravujú viaceré bezpečnostné zraniteľnosti.

Najvážnejšia bezpečnostná zraniteľnosť v produkte IGSS SCADA je spôsobená nedostatočnou implementáciu mechanizmov ochrany pamäte a lokálny útočník by ju mohol zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služieb.

Zraniteľnosť v produkte StruxureOn Gateway by vzdialený neautentifikovaný útočník mohol prostredníctvom uploadu špeciálne upraveného *.zip* súboru zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad napadnutým systémom.

Dátum prvého zverejnenia varovania

06.02.2018

CVE

CVE-2017-9967, CVE-2017-9968, CVE-2017-9969, CVE-2017-9970

Zasiahnuté systémy

IGSS SCADA Software V12 a všetky predchádzajúce verzie
StruxureOn Gateway 1.0.0, 1.1.0
IGSS Mobile pre Android verzia 3.01 a staršie
IGSS Mobile pre iOS verzia 3.01 a staršie

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.schneider-electric.com/en/download/document/SEVD-2018-037-01/
https://ics-cert.us-cert.gov/advisories/ICSA-18-044-02
https://nvd.nist.gov/vuln/detail/CVE-2017-9967
https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Id=9105033564&p_File_Name=SEVD-2018-039-01+Struxureon+Gateway.pdf&p_Reference=SEVD-2018-039-01

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

Identifikátor

Bugzilla report.cgi Cross-Site Request Forgery Vulnerability

Popis

Produkt Bugzilla obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia URL odkazu zneužiť na eskaláciu privilégií a neoprávnený prístup k citlivým údajom.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov vo funkcii *report.cgi*, ktorá umožňuje vykonanie CSRF (Cross-Site Request Forgery) útoku.

Dátum prvého zverejnenia varovania

19.02.2018

CVE

CVE-2018-5123

Zasiahnuté systémy

Bugzilla verzie 2.16rc1 až 4.4.12, 4.5.1 až 5.0.3

Následky

Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://bugzilla.mozilla.org/show_bug.cgi?id=1433400
https://www.securitytracker.com/id/1040389
https://tools.cisco.com/security/center/viewAlert.x?alertId=56863