BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 11. 2019 - 26. 11. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Jenkins plugins viacero zraniteľností	Vysoká	**8.8**
02.	Zraniteľnosť Outlook pre Android	Vysoká	**8.7**
03.	IBM Security Identity Manager zraniteľnosť	Vysoká	**8.0**
04.	HP ThinPro zraniteľnosti	Vysoká	**7.6**
05.	BIND zraniteľnosť	Vysoká	**7.5**
06.	Pivotal RabbitMQ zraniteľnosti	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 2915

SK-CERT
Naša značka:
01380/2019/SK-CERT-275

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

Identifikátor

Jenkins plugins viacero zraniteľností

Popis

Vývojári produktu Jenkins informovali o bezpečnostných zraniteľnostiach vo viacerých zásuvných moduloch.
Najvážnejšia bezpečnostná zraniteľnosť v Script Security Plugin je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.11.2019

CVE

CVE-2019-16538, CVE-2019-16539, CVE-2019-16540, CVE-2019-16541, CVE-2019-16542, CVE-2019-16543, CVE-2019-16544, CVE-2019-16545, CVE-2019-16546, CVE-2019-16547, CVE-2019-16548

Zasiahnuté systémy

Anchore Container Image Scanner Plugin verzie staršie ako 1.0.20
Google Compute Engine Plugin verzie staršie ako 4.2.0
JIRA Plugin verzie staršie ako 3.0.11
QMetry for JIRA - Test Management Plugin verzia 1.13 a staršie
Script Security Plugin verzie staršie ako 1.68
Spira Importer Plugin verzie staršie ako 3.2.3
Support Core Plugin verzie staršie ako 2.64

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade pluginov, na ktoré doposiaľ neboli vydané aktualizácie administrátorom odporúčame zvážiť ich odinštalovanie a tiež sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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://jenkins.io/security/advisory/2019-11-21/
https://exchange.xforce.ibmcloud.com/vulnerabilities/172025
https://exchange.xforce.ibmcloud.com/vulnerabilities/172028
https://exchange.xforce.ibmcloud.com/vulnerabilities/172029

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.7**
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 je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej e-mailovej správy získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

19.11.2019

CVE

CVE-2019-1460

Zasiahnuté systémy

Outlook pre Android verzie staršie ako 4.0.65

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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-2019-1460
https://threatpost.com/microsoft-outlook-android-bug-xss/150528/

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

Identifikátor

IBM Security Identity Manager zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Security Access Manager, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.11.2019

CVE

CVE-2019-4561

Zasiahnuté systémy

IBM Security Identity Manager verzie staršie ako 6.0.0.22-ISS-SIM-IF0001

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.ibm.com/support/pages/node/1108695
https://exchange.xforce.ibmcloud.com/vulnerabilities/166456

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.6**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

HP ThinPro zraniteľnosti

Popis

Spoločnosť HP vydala bezpečnostnú aktualizáciu na svoj produkt HP ThinPro, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.11.2019

CVE

CVE-2019-16285, CVE-2019-16286, CVE-2019-16287, CVE-2019-18909, CVE-2019-18910

Zasiahnuté systémy

HP ThinPro verzie staršie ako 7.1 Service Pack 4

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
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://support.hp.com/us-en/document/c06509350
https://nvd.nist.gov/vuln/detail/CVE-2019-18909

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

Identifikátor

BIND zraniteľnosť

Popis

Vývojári DNS servera BIND vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť vo funkcionalite TCP-pipelining je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

20.11.2019

CVE

CVE-2019-6477

Zasiahnuté systémy

BIND verzie staršie ako 9.11.13-S1, 9.11.13, 9.14.8 a 9.15.6

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Administrátorom tiež odporúčame zvážiť deaktiváciu funkcie TCP-pipelining.

Zdroje

https://kb.isc.org/docs/cve-2019-6477
https://exchange.xforce.ibmcloud.com/vulnerabilities/172012

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

Identifikátor

Pivotal RabbitMQ zraniteľnosti

Popis

Spoločnosť Pivotal vydala bezpečnostnú aktualizáciu na svoj produkt RabbitMQ , ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

22.11.2019

CVE

CVE-2019-11287, CVE-2019-11291

Zasiahnuté systémy

Pivotal RabbitMQ verzie staršie ako v3.7.21, v3.8.1, 1.17.4 a 1.16.7

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://pivotal.io/security/cve-2019-11287
https://pivotal.io/security/cve-2019-11291
https://nvd.nist.gov/vuln/detail/CVE-2019-11291
https://nvd.nist.gov/vuln/detail/CVE-2019-11287