BEZPEČNOSTNÝ BULLETIN

Týždeň 25. 11. 2020 - 01. 12. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Zraniteľnosti v PC Analyser application	Vysoká	**8.8**
02.	Bezpečnostná zraniteľnosť Drupal	Vysoká	**7.8**
03.	Zraniteľnosť v knižnici libslirp	Vysoká	**7.5**
04.	Zraniteľnosť v platforme Moodle	Vysoká	**7.3**
05.	Zraniteľnosť v Huawei ManageOne	Vysoká	**7.2**
06.	Viacero zraniteľností v systéme na zdieľanie dát GROWI	Vysoká	**7.2**
07.	Zraniteľnosti v balíku Teclib GLPI	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:
01439/2020/SK-CERT-276

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

Identifikátor

Zraniteľnosti v PC Analyser application

Popis

Spoločnosť David Espenschield Software vydala bezpečnostnú aktualizáciu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia zraniteľnosť sa nachádza v driveri PCADRVX64.sys, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.11.2020

CVE

CVE-2020-28921, CVE-2020-28922

Zasiahnuté systémy

PC Analyser application by Devid Espenschied Software verzie staršie ako 4.10

Následky

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

Odporúčania

Administrátorom a používateľom 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://github.com/eset/vulnerability-disclosures/blob/master/CVE-2020-28921/CVE-2020-28921.md
https://github.com/eset/vulnerability-disclosures/blob/master/CVE-2020-28922/CVE-2020-28922.md

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

Identifikátor

Bezpečnostná zraniteľnosť Drupal

Popis

Spoločnosť Drupal vydala bezpečnostnú aktualizáciu na svoj systém pre manažment webstránok Drupal, ktorá opravuje dve bezpečnostné zraniteľnosti v knižnici PEAR Archive_Tar.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.11.2020

CVE

CVE-2020-28948, CVE-2020-28949

Zasiahnuté systémy

Drupal 7 verzie staršie ako 7.75
Drupal 8 verzie staršie ako 8.8.12
Drupal 8 verzie staršie ako 8.9.10
Drupal 9 verzie staršie ako 9.0.9

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na platforme Drupal. V prípade, že áno, 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.drupal.org/sa-core-2020-013
https://github.com/pear/Archive_Tar/issues/33

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

Identifikátor

Zraniteľnosť v knižnici libslirp

Popis

Vývojári knižnice libslirp vydali bezpečnostnú aktualizáciu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Obe zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

26.11.2020

CVE

CVE-2020-29129, CVE-2020-29130

Zasiahnuté systémy

Slirp libslirp verzie staršie ako 2.28.0

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://lists.freedesktop.org/archives/slirp/2020-November/000115.html
https://seclists.org/oss-sec/2020/q4/167
https://exchange.xforce.ibmcloud.com/vulnerabilities/192365
https://exchange.xforce.ibmcloud.com/vulnerabilities/192366

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v platforme Moodle

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti vo výučbovej platforme Moodle.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.11.2020

CVE

Zasiahnuté systémy

Moodle verzie staršie ako 3.8 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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.exploit-db.com/exploits/49114
https://exchange.xforce.ibmcloud.com/vulnerabilities/192381

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

Identifikátor

Zraniteľnosť v Huawei ManageOne

Popis

Spoločnosť Huawei vydala bezpečnostnú aktualizáciu na svoj produkt ManageOne, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi s administrátorskými právomocami prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.11.2020

CVE

CVE-2020-9115

Zasiahnuté systémy

Huawei ManageOne verzie staršie ako 8.0.2

Následky

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

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://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201125-01-commandinjection-en

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

Identifikátor

Viacero zraniteľností v systéme na zdieľanie dát GROWI

Popis

Spoločnosť GROWI vydala bezpečnostnú aktualizáciu na svoj produkt growi.cloud, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov umožňuje vzdialenému, autentifikovanému útočníkovi získať prístup k citlivým údajom alebo vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

25.11.2020

CVE

CVE-2020-5676, CVE-2020-5677, CVE-2020-5678

Zasiahnuté systémy

GROWI 4.1.5

Následky

Vykonanie škodlivého kódu
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

http://jvn.jp/en/jp/JVN56450373/index.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/192345
https://exchange.xforce.ibmcloud.com/vulnerabilities/192344
https://exchange.xforce.ibmcloud.com/vulnerabilities/192346

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

Identifikátor

Zraniteľnosti v balíku Teclib GLPI

Popis

Vývojári balíka na IT manažment GLPI vydali bezpečnostnú aktualizáciu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Obe zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky získať neoprávený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

25.11.2020

CVE

CVE-2020-27662, CVE-2020-27663

Zasiahnuté systémy

GLPI verzie staršie ako 9.5.3

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.

Zdroje

https://github.com/glpi-project/glpi/security/advisories/GHSA-pqfv-4pvr-55r4
https://exchange.xforce.ibmcloud.com/vulnerabilities/192360
https://exchange.xforce.ibmcloud.com/vulnerabilities/192359