BEZPEČNOSTNÝ BULLETIN

Týždeň 19. 01. 2022 - 25. 01. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	AIDE - bezpečnostná zraniteľnosť	Vysoká	**8.4**
02.	WordPress Email Template Designer - bezpečnostná zraniteľnosť	Vysoká	**8.3**
03.	McAfee Agent - dve bezpečnostné zraniteľnosti	Vysoká	**7.8**
04.	USBView - bezpečnostná zraniteľnosť	Vysoká	**7.8**
05.	Linuxový komponent polkit - bezpečnostná zraniteľnosť 'PwnKit'	Vysoká	**7.8**
06.	Sidekiq - bezpečnostná zraniteľnosť	Vysoká	**7.5**
07.	util-linux - bezpečnostná zraniteľnosť	Vysoká	**7.1**

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:
01794/2022/SK-CERT-660

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

Identifikátor

AIDE - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja AIDE vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.01.2022

CVE

CVE-2021-45417

Zasiahnuté systémy

AIDE vo verzii staršej ako 0.17.4

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://seclists.org/oss-sec/2022/q1/59
https://github.com/aide/aide/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45417
https://exchange.xforce.ibmcloud.com/vulnerabilities/217807

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

Identifikátor

WordPress Email Template Designer - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu WordPress Email Template Designer vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

19.01.2022

CVE

CVE-2022-0218

Zasiahnuté systémy

WordPress Email Template Designer vo verzii staršej ako 3.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Pri webových stránkach odporúčame zvážiť možnosť prevádzkovať redakčný systém nedostupný z verejného internetu a na verejný prezentačný server nahrávať len vyexportovanú statickú verziu stránky.
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://www.wordfence.com/blog/2022/01/unauthenticated-xss-vulnerability-patched-in-html-email-template-designer-plugin/
https://thehackernews.com/2022/01/hackers-planted-secret-backdoor-in.html
https://threatpost.com/wordpress-insecure-plugin-rest-api/177866/

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

Identifikátor

McAfee Agent - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť McAfee vydala bezpečnostnú aktualizáciu na svoj produkt McAfee Agent, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvoreného súboru, eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.01.2022

CVE

CVE-2021-31854, CVE-2022-0166

Zasiahnuté systémy

McAfee Agent vo verzii staršej ako 5.7.5

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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://kc.mcafee.com/corporate/index?page=content&id=SB10378
https://cybersafe.news/mcafee-agent-bug-exploited-to-gain-windows-system-privileges/
https://threatpost.com/mcafee-bug-windows-system-privileges/177857/
https://nvd.nist.gov/vuln/detail/CVE-2022-0166

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

Identifikátor

USBView - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja USBView vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.01.2022

CVE

CVE-2022-23220

Zasiahnuté systémy

USBView vo verzii staršej ako 2.2

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://seclists.org/oss-sec/2022/q1/61
https://github.com/gregkh/usbview/commit/38e9dc56a437721f7a8b0ec1d2b4e611e090c87d
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23220
https://exchange.xforce.ibmcloud.com/vulnerabilities/217898

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

Identifikátor

Linuxový komponent polkit - bezpečnostná zraniteľnosť 'PwnKit'

Popis

Vývojári linuxového komponentu polkit vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť. Uvedená komponenta polkit je štadardne nainštalovaná vo všetkých hlavných linuxvých distribúciách.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zraniteľnosť je možné zneužiť aj v prípade, že na systéme nie je spustený samotný démon polkit.

Dátum prvého zverejnenia varovania

25.01.2022

CVE

CVE-2021-4034

Zasiahnuté systémy

pkexec vo verzii staršej ako commit a2bf5c9c
Ubuntu 21.10 (Impish Indri) vo verzii staršej ako 0.105-31ubuntu0.1
Ubuntu 20.04 LTS (Focal Fossa) vo verzii staršej ako 0.105-26ubuntu1.2
Ubuntu 18.04 LTS (Bionic Beaver) vo verzii staršej ako 0.105-20ubuntu0.18.04.6
Ubuntu 16.04 ESM (Xenial Xerus) vo verzii staršej ako 0.105-14.1ubuntu0.5+esm1
Ubuntu 14.04 ESM (Trusty Tahr) vo verzii staršej ako 0.105-4ubuntu3.14.04.6+esm1
Debian vo verzii staršej ako 0.105-18+deb9u2
Debian vo verzii staršej ako 0.105-31+deb11u1
Debian vo verzii staršej ako 0.105-25+deb10u1
Debian vo verzii staršej ako 0.105-31.1
Red Hat Enterprise Linux 6 Extended Lifecycle Support
Red Hat Enterprise Linux 7
Red Hat Enterprise Linux 7.3
Red Hat Enterprise Linux 7.4
Red Hat Enterprise Linux 7.6
Red Hat Enterprise Linux 7.6
Red Hat Enterprise Linux 7.6
Red Hat Enterprise Linux 7.7
Red Hat Enterprise Linux 7.7
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://access.redhat.com/security/cve/CVE-2021-4034

Následky

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL). Ak výrobca ešte nevydal aktualizáciu operačného systému, ktorý túto zraniteľnosť opravuje, odporúčame ako dočasnú mitigáciu odstrániť SUID-bit z pkexec (napríklad príkazom chmod 0755 /usr/bin/pkexec). 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.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt https://gitlab.freedesktop.org/polkit/polkit/-/commit/a2bf5c9c83b6ae46cbd5c779d3055bff81ded683 https://access.redhat.com/security/cve/CVE-2021-4034 https://vulmon.com/vulnerabilitydetails?qid=CVE-2021-4034 https://thehackernews.com/2022/01/12-year-old-polkit-flaw-lets.html https://www.sk-cert.sk/sk/varovanie-zranitelnost-v-distribuciach-linuxu/

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

Identifikátor

Sidekiq - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Sidekiq vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.01.2022

CVE

CVE-2022-23837

Zasiahnuté systémy

Sidekiq vo verzii staršej ako 6.4.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/mperham/sidekiq/commit/7785ac1399f1b28992adb56055f6acd88fd1d956
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23837
https://exchange.xforce.ibmcloud.com/vulnerabilities/218003

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

util-linux - bezpečnostná zraniteľnosť

Popis

Vývojári knižnice util-linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

24.01.2022

CVE

CVE-2021-3996

Zasiahnuté systémy

util-linux vo verzii staršej ako 2.37

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://seclists.org/oss-sec/2022/q1/66
https://github.com/util-linux/util-linux/commits/stable/v2.37
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3996
https://exchange.xforce.ibmcloud.com/vulnerabilities/217979

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:
01794/2022/SK-CERT-660