BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 01. 2022 - 18. 01. 2022

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:
01794/2022/SK-CERT-657

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

Identifikátor

Woocommerce pluginy pre Wordpress - bezpečnostná zraniteľnosť

Popis

Vývojári pluginov Login/Signup Popup, Waitlist Woocommerce a Side Cart Woocommerce vydali bezpečnostnú aktualizáciu svojich produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov 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

13.01.2022

CVE

CVE-2022-0215

Zasiahnuté systémy

Login/Signup Popup vo verzii staršej ako 2.3
Waitlist Woocommerce vo verzii staršej ako 2.5.2
Side Cart Woocommerce vo verzii staršej ako 2.1

Následky

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

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.
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://thehackernews.com/2022/01/high-severity-vulnerability-in-3.html https://www.wordfence.com/blog/2022/01/84000-wordpress-sites-affected-by-three-plugins-with-the-same-vulnerability/?utm_medium=email&_hsmi=200773868&_hsenc=p2ANqtz-8wONqcLAiQD8o__3dsSDSjuLwHX4hhqMgH_Vvhs-LcUGTU2JWYOvVeflfGHs_Uz1VP67vtVIWObFp9507lPzgx4OjFww&utm_content=200773868&utm_source=hs_email https://threatpost.com/plugins-vulnerability-84k-wordpress-sites/177654/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

GitLab - viacero bezpečnostných zraniteľností

Popis

Vývojári nástroja GitLab vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

11.01.2022

CVE

CVE-2021-39927, CVE-2021-39942, CVE-2021-39946, CVE-2022-0090, CVE-2022-0093, CVE-2022-0124, CVE-2022-0125, CVE-2022-0151, CVE-2022-0152, CVE-2022-0154, CVE-2022-0172

Zasiahnuté systémy

GitLab Community Edition 14.6.2
GitLab Community Edition 14.5.3
GitLab Community Edition 14.4.5
GitLab Enterprise Edition 14.6.2
GitLab Enterprise Edition 14.5.3
GitLab Enterprise Edition 14.4.5

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://about.gitlab.com/releases/2022/01/11/security-release-gitlab-14-6-2-released/
https://portswigger.net/daily-swig/gitlab-shifts-left-to-patch-high-impact-vulnerabilities

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

Identifikátor

Adobe produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.01.2022

CVE

CVE-2021-44702, CVE-2021-44704, CVE-2021-44706, CVE-2021-45057

Zasiahnuté systémy

Adobe InDesign vo verzii staršej ako 16.4.1
Adobe Acrobat DC vo verzii staršej ako 21.011.20039
Adobe Acrobat Reader DC vo verzii staršej ako 21.011.20039
Adobe Acrobat 2020 vo verzii staršej ako 20.004.30020
Adobe Acrobat Reader 2020 vo verzii staršej ako 20.004.30020
Adobe Acrobat 2017 vo verzii staršej ako 17.011.30207
Adobe Acrobat Reader 2017 vo verzii staršej ako 17.011.30207

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje
https://helpx.adobe.com/security/products/indesign/apsb22-05.html
https://helpx.adobe.com/security/products/acrobat/apsb22-01.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45057
https://exchange.xforce.ibmcloud.com/vulnerabilities/217008
https://www.securityweek.com/adobe-patches-reader-flaws-earned-hackers-150000-chinese-contest

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Juniper Networks Junos OS a CSO produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Juniper Networks vydala bezpečnostné aktualizácie na produkty Junos OS a CSO, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

12.01.2022

CVE

CVE-2022-22152, CVE-2022-22153

Zasiahnuté systémy

Juniper Networks CSO vo verzii staršej ako 6.1.0 Patch 3
Juniper Networks Junos OS 17.3 vo verzii staršej ako 17.3R3-S12;
Juniper Networks Junos OS 17.4 vo verzii staršej ako 17.4R3-S5;
Juniper Networks Junos OS 18.4 vo verzii staršej ako 18.4R2-S10, 18.4R3-S10;
Juniper Networks Junos OS 19.1 vo verzii staršej ako 19.1R3-S8;
Juniper Networks Junos OS 19.2 vo verzii staršej ako 19.2R1-S8, 19.2R3-S4;
Juniper Networks Junos OS 19.3 vo verzii staršej ako 19.3R3-S3;
Juniper Networks Junos OS 19.4 vo verzii staršej ako 19.4R3-S5;
Juniper Networks Junos OS 20.1 vo verzii staršej ako 20.1R3-S1;
Juniper Networks Junos OS 20.2 vo verzii staršej ako 20.2R3-S2;
Juniper Networks Junos OS 20.3 vo verzii staršej ako 20.3R3-S1;
Juniper Networks Junos OS 20.4 vo verzii staršej ako 20.4R2-S2, 20.4R3;
Juniper Networks Junos OS 21.1 vo verzii staršej ako 21.1R2-S2, 21.1R3;
Juniper Networks Junos OS 21.2 vo verzii staršej ako 21.2R2

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://kb.juniper.net/InfoCenter/index?page=content&id=JSA11260&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11261&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11265&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11267&cat=SIRT_1&actp=LIST

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

Identifikátor

Mitsubishi Electric MELSEC-F produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostné aktualizácie na produkty série MELSEC-F, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorených paketov, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.01.2022

CVE

CVE-2021-20612, CVE-2021-20613

Zasiahnuté systémy

FX3U-ENET s firmware vo verzii staršej ako 1.17
FX3U-ENET-L s firmware vo verzii staršej ako 1.17
FX3U-ENET-P502 s firmware vo verzii staršej ako 1.17

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-013-01
https://www.cisa.gov/uscert/ics/advisories/icsa-22-013-07

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

Identifikátor

Apple HomeKit - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na produkty iOS a iPadOS, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

12.01.2022

CVE

CVE-2022-22588

Zasiahnuté systémy

iOS vo verzii staršej ako 15.2.1
iPadOS vo verzii staršej ako 15.2.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://support.apple.com/en-us/HT213043
https://thehackernews.com/2022/01/apple-releases-iphone-and-ipad-updates.html
https://thehackernews.com/2022/01/researchers-detail-new-homekit-doorlock.html