BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 11. 2021 - 30. 11. 2021

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:
01439/2020/SK-CERT-625

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

Identifikátor

Foxit PhantomPDF - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Foxit vydala bezpečnostnú aktualizáciu na svoj produkt PhantomPDF, ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného PDF súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.11.2021

CVE

CVE-2021-34948, CVE-2021-34949, CVE-2021-34950, CVE-2021-34951, CVE-2021-34952, CVE-2021-34953, CVE-2021-34954, CVE-2021-34955, CVE-2021-34956, CVE-2021-34957, CVE-2021-34958, CVE-2021-34959, CVE-2021-34960, CVE-2021-34961, CVE-2021-34962, CVE-2021-34963, CVE-2021-34964, CVE-2021-34965, CVE-2021-34966, CVE-2021-34967, CVE-2021-34968, CVE-2021-34969, CVE-2021-34970, CVE-2021-34971, CVE-2021-34972, CVE-2021-34973, CVE-2021-34974, CVE-2021-34975, CVE-2021-34976, CVE-2021-40326, CVE-2021-41780, CVE-2021-41781, CVE-2021-41782, CVE-2021-41783, CVE-2021-41784, CVE-2021-41785

Zasiahnuté systémy

Foxit PhantomPDF vo verzii staršej ako 10.1.6

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.foxit.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PhantomPDF+10.1.62021-11-29+00%3A00%3A00

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

Identifikátor

Aim produkt - bezpečnostná zraniteľnosť

Popis

Vývojári produktu Aim vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.11.2021

CVE

CVE-2021-43775

Zasiahnuté systémy

Aim vo verzii staršej ako 3.1.0

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/aimhubio/aim/security/advisories/GHSA-8phj-f9w2-cjcc
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43775
https://exchange.xforce.ibmcloud.com/vulnerabilities/213983

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

HejHome GKW-IC052 IP Camera - bezpečnostná zraniteľnosť

Popis

Spoločnosť HejHome vydala bezpečnostnú aktualizáciu na IP kameru GKW-IC052, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.11.2021

CVE

CVE-2021-26611

Zasiahnuté systémy

HejHome GKW-IC052 vo verzii staršej ako 4.0.7

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.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=36359
https://www.hej.life/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26611
https://exchange.xforce.ibmcloud.com/vulnerabilities/214128

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

Identifikátor

Bandisoft ARK Library - bezpečnostná zraniteľnosť

Popis

Spoločnosť Bandisoft vydala bezpečnostnú aktualizáciu na produkt ARK library, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.11.2021

CVE

CVE-2021-26615

Zasiahnuté systémy

Bandisoft ARK library vo verzii staršej ako 7.16.0.1

Následky

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

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 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://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=36361
https://kr.bandisoft.com/ark/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26615
https://exchange.xforce.ibmcloud.com/vulnerabilities/214129

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

Identifikátor

ImageMagick produkt - bezpečnostná zraniteľnosť

Popis

Vývojári produktu ImageMagick vydali bezpečnostnú aktualizáciu na produkt ImageMagick, ktorá opravuje bezpečnostnú zraniteľnosť. 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

23.11.2021

CVE

CVE-2021-3962

Zasiahnuté systémy

ImageMagick vo verzii staršej ako 7.1.0-15

Následky

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

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 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://bugzilla.redhat.com/show_bug.cgi?id=2023196
https://github.com/ImageMagick/ImageMagick/issues/4446
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3962
https://exchange.xforce.ibmcloud.com/vulnerabilities/213990

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

Identifikátor

Quagga produkt - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti produktu Quagga. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na zraniteľnosť v súčasnosti neexistujú bezpečnostné aktualizácie. Úspešné zneužitie zraniteľnosti vyžaduje kombináciu viacerých faktorov, preto závažnosť závisí od konkrétnej inštalácie.

Dátum prvého zverejnenia varovania

22.11.2021

CVE

CVE-2021-44038

Zasiahnuté systémy

Quagga Quagga vo verzii staršej ako 1.2.4 (vrátane)

Následky

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

Odporúčania

Vzhľadom k tomu, že projekt Quagga nie je aktívny a je pravdepodobné, že bezpečnostné aktualizácie nebudú vydané, odporúčame zvážiť náhradu existujúcich inštalácií iným produktom.
Administrátorom a používateľom odporúčame sledovať stránku 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://bugzilla.suse.com/show_bug.cgi?id=1191890
https://github.com/Quagga/quagga
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44038
https://exchange.xforce.ibmcloud.com/vulnerabilities/213935

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

Identifikátor

AfreecaTV produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť AfreecaTV vydala bezpečnostnú aktualizáciu na produkt AfreecaTV, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii strcpy(). Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, 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

25.11.2021

CVE

CVE-2020-7881

Zasiahnuté systémy

AfreecaTV vo verzii staršej ako 2020.09.24

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://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=36357
https://afreecatv.com/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7881
https://exchange.xforce.ibmcloud.com/vulnerabilities/214125

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

Identifikátor

VMware vCenter Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na produkt vCenter Server, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.11.2021

CVE

CVE-2021-21980

Zasiahnuté systémy

VMware vCenter Server 6.7 U3p
VMware vCenter Server 6.5 U3r

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

Zdroje

https://www.vmware.com/security/advisories/VMSA-2021-0027.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21980
https://exchange.xforce.ibmcloud.com/vulnerabilities/213975

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

Identifikátor

Apache APISIX - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na produkt APISIX, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.11.2021

CVE

CVE-2021-43557

Zasiahnuté systémy

Apache APISIX vo verzii staršej ako 2.10.2

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://seclists.org/oss-sec/2021/q4/124
https://seclists.org/oss-sec/2021/q4/125
https://apisix.apache.org/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43557
https://exchange.xforce.ibmcloud.com/vulnerabilities/213889