



OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	PostgreSQL - bezpečnostná zraniteľnosť	Vysoká	8.8
02.	Apache Tomcat - bezpečnostná zraniteľnosť	Vysoká	8.6
03.	SonicWall produkty - viacero bezpečnostných zraniteľností	Vysoká	8.2
04.	Delta Electronics CNCSoft produkt - dve bezpečnostné zraniteľnosti	Vysoká	7.8
05.	Inkscape - viacero bezpečnostných zraniteľností	Vysoká	7.8
06.	Foxit PDF Reader - bezpečnostná zraniteľnosť	Vysoká	7.8



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

PostgreSQL - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja PostgreSQL vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami privilegovaného používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.05.2022

CVE

CVE-2022-1552

Zasiahnuté systémy

PostgreSQL vo verzii staršej ako 10.21

PostgreSQL vo verzii staršej ako 11.16

PostgreSQL vo verzii staršej ako 12.11

PostgreSQL vo verzii staršej ako 13.7

PostgreSQL vo verzii staršej ako 14.3

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

V prípade, že aktualizácia systému nie je možná, tak vývojári nástroja odporúčajú zakázať funkcionality autovacuum a neobnovovať zálohy prostredníctvom príkazu `pg_dump`.

Odporúčame uistiť sa, či Vaše aplikácie interne nevyužívajú PostgreSQL v zraniteľnej verzii.

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.postgresql.org/support/security/CVE-2022-1552/>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1552>
<https://exchange.xforce.ibmcloud.com/vulnerabilities/226521>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.6
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Apache Tomcat - bezpečnostná zraniteľnosť

Popis

Nadácia Apache vydalo bezpečnostnú aktualizáciu na svoj produkt Tomcat, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepřístupnenie služby.

Dátum prvého zverejnenia varovania

12.05.2022

CVE

CVE-2022-25762

Zasiiahnuté systémy

Apache Tomcat vo verzii staršej ako 9.0.21

Apache Tomcat vo verzii staršej ako 8.5.76

Následky

Neoprávnený prístup k citlivým údajom

Neoprávnená zmena v systéme

Znepřístupnenie služby

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://lists.apache.org/thread/qzqkqh2819x6zsmj7vwdf14ng2fdgkw7>

<https://access.redhat.com/security/cve/cve-2022-25762>

<https://www.cisa.gov/uscert/ncas/current-activity/2022/05/16/apache-releases-security-advisory-tomcat>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.2
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

SonicWall produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť SonicWall vydala bezpečnostnú aktualizáciu na produkty série SMA, ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

13.05.2022

CVE

CVE-2022-1701, CVE-2022-1702, CVE-2022-22282

Zasiiahnuté systémy

SonicWall SMA1000 vo verzii staršej ako 12.4.1-02994
SonicWall SMA 6200, 6210, 7200, 7210, 8000v (ESX, KVM, Hyper-V, AWS, Azure) vo verzii staršej ako 12.4.1-02994

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiiahnutých 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://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0009>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22282>
<https://exchange.xforce.ibmcloud.com/vulnerabilities/226489>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Delta Electronics CNCSoft produkt - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na produkt CNCSoft, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.05.2022

CVE

CVE-2022-1404, CVE-2022-1405

Zasiahnuté systémy

CNCSoft vo verzii staršej ako 1.01.32

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 lokálne 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 administratívnejmu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

<https://us-cert.cisa.gov/ics/advisories/icsa-22-132-01>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Inkscape - viacero bezpečnostných zraniteľností

Popis

Vývojári nástroja Inkscape vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia 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

12.05.2022

CVE

CVE-2021-42700, CVE-2021-42702, CVE-2021-42704

Zasiiahnuté systémy

Inkscape vo verzii staršej ako 1.0

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 lokálne 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 administratívnejmu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje<https://us-cert.cisa.gov/ics/advisories/icsa-22-132-03>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Foxit PDF Reader - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Foxit PDF Reader vydali bezpečnostnú aktualizáciu svojho produktu, 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

12.05.2022

CVE

CVE-2022-28671

Zasiahnuté systémy

Foxit PDF Reader vo verzii staršej ako 11.2.2

Foxit PDF Editor vo verzii staršej ako 11.2.2

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 lokálne 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.

Zdroje

<https://www.zerodayinitiative.com/advisories/ZDI-22-762/>

<https://www.foxit.com/support/security-bulletins.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28671>

<https://exchange.xforce.ibmcloud.com/vulnerabilities/226454>