BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 01. 2024 - 30. 01. 2024

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-1509

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

Identifikátor

Apache Airflow - bezpečnostná zraniteľnosť

Popis

Vývojári platformy Apache Airflow vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prístup ku konfiguračnému súboru Kubernetes, ktorého obsah sa v metadátach a logoch ukladá v nešifrovanej podobe. Údaje získané z tohto súboru môže následne útočník zneužiť na neoprávnený prístup ku Kubernetes clusteru a ďalšie útoky.

Dátum prvého zverejnenia varovania

23.01.2024

CVE

CVE-2023-51702

Zasiahnuté systémy

Apache Airflow CNCF Kubernetes provider vo verzii staršej ako 7.0.0
Apache Airflow vo verzii staršej ako 2.6.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Úplné narušenie dôvernosti, integrity a dostupnosti systému

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/2024/q1/47
https://exchange.xforce.ibmcloud.com/vulnerabilities/280388

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

Identifikátor

Juniper Junos OS produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Juniper vydala bezpečnostnú aktualizáciu na svoje produkty Junos OS a Junos OS Evolved, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2024-21620 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS (Cross-Site Scripting) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.01.2024

CVE

CVE-2023-36846, CVE-2023-36851, CVE-2023-48795, CVE-2024-21619, CVE-2024-21620

Zasiahnuté systémy

Junos OS vo verzii staršej ako 19.4R3-S13, 20.4R3-S10, 21.4R3-S6, 22.1R3-S5, 22.2R3-S3, 22.4R3-S1, 23.2R2, 23.4R2, 24.1R1, 20.4R3-S10*, 21.2R3-S8*, 21.4R3-S6*, 22.1R3-S5*, 22.2R3-S3*, 22.3R3-S2*, 22.4R3-S1*, 23.2R2*, 23.4R2*, 20.4R3-S9, 21.2R3-S7*, 21.3R3-S5, 21.4R3-S6*, 22.1R3-S5*, 22.2R3-S3*, 22.3R3-S2*, 22.4R3*, 23.2R1-S2, 23.2R2*, 23.4R1

Junos OS Evolved vo verzii staršej ako 19.4R3-S13, 20.4R3-S10, 21.4R3-S6, 22.1R3-S5, 22.2R3-S3, 22.4R3-S1, 23.2R2, 23.4R2, 24.1R1

Následky

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

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.

Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://supportportal.juniper.net/s/article/2024-01-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-have-been-addressed?language=en_US

https://supportportal.juniper.net/s/article/2024-01-Reference-Advisory-Junos-OS-and-Junos-OS-Evolved-Impact-of-Terrapin-SSH-Attack-CVE-2023-48795?language=en_US

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

Identifikátor

Trend Micro Security 2023 (Consumer) uiAirSupport - bezpečnostná zraniteľnosť

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoj produkt Trend Micro Security 2023 uiAirSupport, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených DLL súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.01.2024

CVE

CVE-2024-23940

Zasiahnuté systémy

Trend Micro Security 2023 (Consumer) uiAirSupport vo verzii staršej ako 6.0.2103

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.

Zdroje

https://helpcenter.trendmicro.com/en-us/article/tmka-12134

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

Identifikátor

PASvisu a PMI v8xx - dve bezpečnostné zraniteľnosti

Popis

Vývojári programov PASvisu a PMI v8xx vydali bezpečnostnú aktualizáciu svojich produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti s označením CVE-2023-45795 a CVE-2023-45796 by útočník mohol zneužiť na realizáciu stored XSS (Cross-Site Scripting) útokov a získanie úplnej kontroly nad systémom.

Dátum prvého zverejnenia varovania

30.01.2024

CVE

CVE-2023-45795, CVE-2023-45796

Zasiahnuté systémy

PASvisu vo verzii staršej ako 1.14.1
PMI v8xx vo verzii staršej ako 2.0.33992 (vrátane)

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.

Zdroje

https://cert.vde.com/en/advisories/VDE-2023-050/

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

Identifikátor

VMware Tanzu Spring Framework - bezpečnostná zraniteľnosť

Popis

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

Dátum prvého zverejnenia varovania

22.01.2024

CVE

CVE-2024-22233

Zasiahnuté systémy

Spring Framework vo verzii staršej ako 6.0.16.
Spring Framework vo verzii staršej ako 6.1.3.

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú predmetný framework v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.

Zdroje

https://spring.io/security/cve-2024-22233/
https://exchange.xforce.ibmcloud.com/vulnerabilities/280184

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

Identifikátor

Open Social Drupal modul- bezpečnostná zraniteľnosť

Popis

Vývojári modulu Open Social pre redakčný systém Drupal vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
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

24.01.2024

CVE

-

Zasiahnuté systémy

Open Social vo verzii staršej ako 12.0.5

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky založené na redakčnom systéme Drupal nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, administrátorom 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://www.drupal.org/sa-contrib-2024-005
https://exchange.xforce.ibmcloud.com/vulnerabilities/280461

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

Identifikátor

Apache Kylin - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Apache Kylin vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom odpočúvania sieťovej prevádzky získať prihlasovacie údaje uložené v súbore kylin.properties, ktoré môže následne zneužiť a získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Zraniteľnosť je možné zneužiť iba v prípade, že Apache Kylin komunikuje prostredníctvom HTTP protokolu.

Dátum prvého zverejnenia varovania

28.01.2024

CVE

CVE-2023-29055

Zasiahnuté systémy

Apache Kylin vo verzii staršej ako 4.0.4

Následky

Neoprávnený prístup k citlivým údajom
Úplné narušenie dôvernosti, integrity a dostupnosti systému

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/2024/q1/62
https://exchange.xforce.ibmcloud.com/vulnerabilities/280809

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

Identifikátor

Splunk Enterprise - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Splunk vydala bezpečnostnú aktualizáciu na svoj produkt Splunk Enterprise, ktorá opravuje viacero bezpečnostných zraniteľností nachádzajúcich sa v komponentoch Splunk Web a Splunk REST API.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.01.2024

CVE

CVE-2024-23675, CVE-2024-23676, CVE-2024-23677, CVE-2024-23678

Zasiahnuté systémy

Splunk Enterprise 9.0 vo verzii staršej ako 9.0.8
Splunk Enterprise 9.1 vo verzii staršej ako 9.1.3
Splunk Cloud

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Zraniteľnosti v Splunk Cloud monitoruje a priamo aktualizuje výrobca.
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://advisory.splunk.com/advisories/SVD-2024-0108
https://advisory.splunk.com/advisories/SVD-2024-0107
https://advisory.splunk.com/advisories/SVD-2024-0106
https://advisory.splunk.com/advisories/SVD-2024-0105
https://www.securityweek.com/high-severity-vulnerability-patched-in-splunk-enterprise/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

WatchGuard EPDR, Panda AD360 a Panda Dome - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť WatchGuard vydala bezpečnostné aktualizácie na svoje portfólio produktov WatchGuard EPDR, Panda AD360 a Panda Dome, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód na úrovni používateľa SYSTEM s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.01.2024

CVE

CVE-2023-6330, CVE-2023-6331, CVE-2023-6332

Zasiahnuté systémy

WatchGuard EPDR a Panda AD360 vo verzii staršej ako 8.00.22.0023
Panda Dome vo verzii staršej ako 22.02.01

Následky

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

https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00001
https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00002
https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00003
https://news.sophos.com/en-us/2024/01/25/multiple-vulnerabilities-discovered-in-widely-used-security-driver/