BEZPEČNOSTNÝ BULLETIN

Týždeň 31. 08. 2022 - 06. 09. 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-871

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

Identifikátor

NodeBB - bezpečnostná zraniteľnosť

Popis

Vývojári frameworku pre tvorbu diskusných fór NodeBB vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v SSO pluginoch a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.
Úspešné zneužitie zraniteľnosti vyžaduje interakciu autentifikovaného používateľa so stránkou podvrhnutou útočníkom.

Dátum prvého zverejnenia varovania

02.09.2022

CVE

CVE-2022-36076

Zasiahnuté systémy

NodeBB vo verzii staršej ako 1.17.2

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému.

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.
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://exchange.xforce.ibmcloud.com/vulnerabilities/235231
https://github.com/NodeBB/NodeBB/security/advisories/GHSA-xmgg-fx9p-prq6

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

Identifikátor

Aruba AOS-CX - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Aruba Networks vydala bezpečnostnú aktualizáciu na svoj operačný systém AOS-CX, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.08.2022

CVE

CVE-2022-23679, CVE-2022-23680, CVE-2022-23681, CVE-2022-23682, CVE-2022-23683, CVE-2022-23684, CVE-2022-23686, CVE-2022-23687, CVE-2022-23688, CVE-2022-23689, CVE-2022-23690, CVE-2022-23691

Zasiahnuté systémy

AOS-CX 10000 Switch Series
AOS-CX 9300 Switch Series
AOS-CX 8400 Switch Series
AOS-CX 8360 Switch Series
AOS-CX 8325 Switch Series
AOS-CX 8320 Switch Series
AOS-CX 6400 Switch Series
AOS-CX 6300 Switch Series
AOS-CX 6200F Switch Series
AOS-CX 6100 Switch Series
AOS-CX 6000 Switch Series
AOS-CX 4100i Switch Series
vo firmvérových verziách
AOS-CX 10.10.xxxx: 10.10.0002 a staršej
AOS-CX 10.09.xxxx: 10.09.1020 a staršej
AOS-CX 10.08.xxxx: 10.08.1060 a staršej
AOS-CX 10.06.xxxx: 10.06.0200 a staršej

Následky

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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04363en_us

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

Identifikátor

Trend Micro Security - bezpečnostná zraniteľnosť

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoj produkt Trend Micro Security, ktorá opravuje bezpečnostnú zraniteľnosť.
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.

Dátum prvého zverejnenia varovania

31.08.2022

CVE

CVE-2022-34893

Zasiahnuté systémy

Trend Micro Security vo verzii staršej ako 17.7

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.zerodayinitiative.com/advisories/ZDI-22-1175/
https://helpcenter.trendmicro.com/en-us/article/tmka-11053

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

Identifikátor

Red Hat Enterprise Linux 7 - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Red Hat vydala bezpečnostnú aktualizáciu na svoj operačný systém Enterprise Linux, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia 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

22.08.2022

CVE

CVE-2022-2738, CVE-2022-2739

Zasiahnuté systémy
Red Hat Enterprise Linux Server 7 SRPM vo verzii staršej ako podman-1.6.4-36.el7_9.src.rpm Red Hat Enterprise Linux Server 7 x86_64 vo verzii staršej ako podman-1.6.4-36.el7_9.x86_64.rpm Red Hat Enterprise Linux Server 7 x86_64 vo verzii staršej ako podman-debuginfo-1.6.4-36.el7_9.x86_64.rpm Red Hat Enterprise Linux Server 7 x86_64 vo verzii staršej ako podman-docker-1.6.4-36.el7_9.noarch.rpm Red Hat Enterprise Linux Workstation 7 SRPM vo verzii staršej ako podman-1.6.4-36.el7_9.src.rpm Red Hat Enterprise Linux Workstation 7 x86_64 vo verzii staršej ako podman-1.6.4-36.el7_9.x86_64.rpm Red Hat Enterprise Linux Workstation 7 x86_64 vo verzii staršej ako podman-debuginfo-1.6.4-36.el7_9.x86_64.rpm Red Hat Enterprise Linux Workstation 7 x86_64 vo verzii staršej ako podman-docker-1.6.4-36.el7_9.noarch.rpm Red Hat Enterprise Linux for IBM z Systems 7 SRPM vo verzii staršej ako podman-1.6.4-36.el7_9.src.rpm Red Hat Enterprise Linux for IBM z Systems 7 s390x vo verzii staršej ako podman-1.6.4-36.el7_9.s390x.rpm Red Hat Enterprise Linux for IBM z Systems 7 s390x vo verzii staršej ako podman-debuginfo-1.6.4-36.el7_9.s390x.rpm Red Hat Enterprise Linux for IBM z Systems 7 s390x vo verzii staršej ako podman-docker-1.6.4-36.el7_9.noarch.rpm Red Hat Enterprise Linux for Power, little endian 7 SRPM vo verzii staršej ako podman-1.6.4-36.el7_9.src.rpm Red Hat Enterprise Linux for Power, little endian 7 ppc64le vo verzii staršej ako podman-1.6.4-36.el7_9.ppc64le.rpm Red Hat Enterprise Linux for Power, little endian 7 ppc64le vo verzii staršej ako podman-debuginfo-1.6.4-36.el7_9.ppc64le.rpm Red Hat Enterprise Linux for Power, little endian 7 ppc64le vo verzii staršej ako podman-docker-1.6.4-36.el7_9.noarch.rpm

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://exchange.xforce.ibmcloud.com/vulnerabilities/235229 https://access.redhat.com/errata/RHSA-2022:6119

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ManageEngine OpManager Plus - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť ManageEngine vydala bezpečnostnú aktualizáciu na svoj produkt OpManager Plus, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v rámci funkcie getDNSResolveOption a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.09.2022

CVE

CVE-2022-37024, CVE-2022-38772

Zasiahnuté systémy

ManageEngine OpManager vo verzii staršej ako 126120,126105,126003,125658

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.zerodayinitiative.com/advisories/ZDI-22-1184/
https://www.manageengine.com/itom/advisory/cve-2022-37024.html