BEZPEČNOSTNÝ BULLETIN

Týždeň 25. 08. 2021 - 31. 08. 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-537

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

Identifikátor

Parallels Desktop produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Parallels vydala bezpečnostnú aktualizáciu na produkt Parallels Desktop, 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

25.08.2021

CVE

CVE-2021-34864

Zasiahnuté systémy

Parallels Parallels Desktop vo verzii staršej ako 17

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade, že chcete zotrvať na verzii Parallels Desktop 16, zakážte funkciu "shared folders" alebo izolujte VM od Mac, ako je opísané na webovej adrese:
https://threatpost.com/parallels-inconvenient-fix/168997/
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.zerodayinitiative.com/advisories/ZDI-21-1000/
https://www.parallels.com/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34864
https://exchange.xforce.ibmcloud.com/vulnerabilities/208188
https://threatpost.com/parallels-inconvenient-fix/168997/

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-537

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

Identifikátor

VMware produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 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, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

24.08.2021

CVE

CVE-2021-22022, CVE-2021-22023, CVE-2021-22024, CVE-2021-22025, CVE-2021-22026, CVE-2021-22027

Zasiahnuté systémy

vRealize Operations Manager 8.5.0
vRealize Operations Manager 8.4.0 vo verzii staršej ako KB85383
vRealize Operations Manager 8.3.0 vo verzii staršej ako KB85382
vRealize Operations Manager 8.2.0 vo verzii staršej ako KB85381
vRealize Operations Manager 8.1.1 vo verzii staršej ako KB85380
vRealize Operations Manager 8.1.0 vo verzii staršej ako KB85380
vRealize Operations Manager 8.0.1 vo verzii staršej ako KB85379
vRealize Operations Manager 8.0.0 vo verzii staršej ako KB85379
vRealize Operations Manager 7.5.0 vo verzii staršej ako KB85378
VMware Cloud Foundation (vROps) 4.x vo verzii staršej ako KB85452
VMware Cloud Foundation (vROps) 3.x vo verzii staršej ako KB85452
vRealize Suite Lifecycle Manager (vROps) 8.x vo verzii staršej ako KB85452

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie 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://www.vmware.com/security/advisories/VMSA-2021-0018.html

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

Identifikátor

Cisco NX-OS a Nexus 9000 séria produktov - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

25.08.2021

CVE

CVE-2021-1523, CVE-2021-1586, CVE-2021-1587, CVE-2021-1588

Zasiahnuté systémy

Nexus 3000 Series Switches (CSCvx66765)
Nexus 7000 Series Switches (CSCvx48078)
Nexus 9000 Series Switches v standalone NX-OS móde (CSCvx66765)
Nexus 9000 Series Fabric Switches v ACI móde
N9K-C9372PX-E
N9K-C9372TX-E
N9K-C9332PQ
N9K-C9372PX
N9K-C9372TX
N9K-C9396PX
N9K-C9396TX
N9K-C93128TX
N9K-C93120TX
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-mpls-oam-dos-sGO9x5GM

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-mpls-oam-dos-sGO9x5GM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9kaci-tcp-dos-YXukt6gM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9kaci-queue-wedge-cLDDEfKF

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

Identifikátor

IBM AIX kernel a VIOS - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na produkty AIX a VIOS, ktorá opravuje bezpečnostnú zraniteľnosť.

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

25.08.2021

CVE

CVE-2021-29801

Zasiahnuté systémy

IBM AIX vo verzii staršej ako 7.1.5 IJ33318
IBM AIX vo verzii staršej ako 7.2.3 IJ32629
IBM AIX vo verzii staršej ako 7.2.4 IJ32630
IBM AIX vo verzii staršej ako 7.2.5 IJ32631
IBM VIOS vo verzii staršej ako 3.1 IJ32629
IBM VIOS vo verzii staršej ako 3.1.1 IJ32630
IBM VIOS vo verzii staršej ako 3.1.2 IJ32631

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.ibm.com/support/pages/node/6483875
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29801
https://exchange.xforce.ibmcloud.com/vulnerabilities/203977

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Johnson Controls CEM Systems AC2000 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na produkt CEM Systems AC2000, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

26.08.2021

CVE

CVE-2021-27663

Zasiahnuté systémy

CEM Systems AC2000 vo verzii staršej ako 10.5 Server Feature Pack 2
CEM Systems AC2000 vo verzii staršej ako 10.6

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-238-01

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

Identifikátor

Delta Electronics TPEditor a DOPSoft produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Delta Electronics vydala bezpečnostné aktualizácie na produkty TPEditor a DOPSoft, ktoré opravujú dve bezpečnostné zraniteľnosti.
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

25.08.2021

CVE

CVE-2021-33007, CVE-2021-33019

Zasiahnuté systémy

TPEditor vo verzii staršej ako v1.98.07
DOPSoft vo verzii staršej ako 4.00.12

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).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-236-03

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

Identifikátor

Hitachi ABB Power Grids Retail Operations a CSB produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hitachi ABB Power Grids vydala bezpečnostnú aktualizáciu na produkty Retail Operations a Counterparty Settlement Billing, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

24.08.2021

CVE

CVE-2021-35529

Zasiahnuté systémy

Retail Operations vo verzii staršej ako 5.7.3
Counterparty Settlement and Billing (CSB) vo verzii staršej ako 5.7.3

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-236-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.3
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Microsoft Exchange Server - bezpečnostná zraniteľnosť 'ProxyToken'

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj produkt Exchange Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

30.08.2021

CVE

CVE-2021-33766

Zasiahnuté systémy

Microsoft Exchange Server 2019 vo verzii staršej ako Cumulative Update 8
Microsoft Exchange Server 2016 vo verzii staršej ako Cumulative Update 19
Microsoft Exchange Server 2013 vo verzii staršej ako Cumulative Update 23
Microsoft Exchange Server 2016 vo verzii staršej ako Cumulative Update 20
Microsoft Exchange Server 2019 vo verzii staršej ako Cumulative Update 9

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-33766
https://thehackernews.com/2021/08/new-microsoft-exchange-proxytoken-flaw.html
https://threatpost.com/microsoft-exchange-proxytoken-email/169030/
https://www.bleepingcomputer.com/news/security/microsoft-exchange-proxytoken-bug-can-let-hackers-steal-user-email/