BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 04. 2021 - 04. 05. 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-406

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

Identifikátor

Cisco FTD Software - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej HTTPS požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.04.2021

CVE

CVE-2021-1402, CVE-2021-1445, CVE-2021-1448, CVE-2021-1493, CVE-2021-1501, CVE-2021-1504

Zasiahnuté systémy

Cisco ASA Software
Cisco FTD Software
3000 Series Industrial Security Appliances (ISAs)
ASA 5512-X Adaptive Security Appliance
ASA 5515-X Adaptive Security Appliance
ASA 5525-X Adaptive Security Appliance
ASA 5545-X Adaptive Security Appliance
ASA 5555-X Adaptive Security Appliance
Firepower 1000 Series
Firepower 2100 Series
Firepower Threat Defense Virtual (FTDv)
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-vpn-dos-fpBcpEcD

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-ssl-decrypt-dos-DdyLuK6c
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-memc-dos-fncTyYKG
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-cmdinj-vWY5wqZT
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-vpn-dos-fpBcpEcD
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-sipdos-GGwmMerC

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

Identifikátor

F5 BIG-IP APM - bezpečnostná zraniteľnosť

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoj produkt BIG-IP APM, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej AS-REP požiadavky eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.04.2021

CVE

CVE-2021-23008

Zasiahnuté systémy

BIG-IP APM vo verzii staršej ako 16.0.1 (vrátane)
BIG-IP APM vo verzii staršej ako 15.1.3
BIG-IP APM vo verzii staršej ako 14.1.4
BIG-IP APM vo verzii staršej ako 13.1.4
BIG-IP APM vo verzii staršej ako 12.1.6
BIG-IP APM vo verzii staršej ako 11.6.5 (vrátane)

Následky

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

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.
Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).
Administrátorom odporúčame nastaviť viac faktorovú autentifikáciu používateľov.

Zdroje

https://support.f5.com/csp/article/K51213246
https://exchange.xforce.ibmcloud.com/vulnerabilities/200885
https://thehackernews.com/2021/04/f5-big-ip-found-vulnerable-to-kerberos.html

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

Identifikátor

VirtualBox pre openSUSE - bezpečnostná zraniteľnosť

Popis

Vývojári programu VirtualBox pre openSUSE vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s používateľskými právomocami, prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.04.2021

CVE

CVE-2021-25319

Zasiahnuté systémy

VirtualBox pre openSUSE vo verzii staršej ako 6.1.18

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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/200757
https://seclists.org/oss-sec/2021/q2/78
https://software.opensuse.org/package/virtualbox

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

Identifikátor

Lenovo PCManager - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Lenovo vydala bezpečnostnú aktualizáciu na svoj produkt PCManager, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s používateľskými právomocami, prostredníctvom podvrhnutia špeciálne vytvoreného DLL súboru, eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.04.2021

CVE

CVE-2021-3451, CVE-2021-3464

Zasiahnuté systémy

Lenovo PCManager vo verzii staršej ako 3.0.400.3252

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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/200864
https://exchange.xforce.ibmcloud.com/vulnerabilities/200861
https://iknow.lenovo.com.cn/detail/dc_196156.html

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

Identifikátor

Foxit Studio Photo - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Foxit vydala bezpečnostnú aktualizáciu na svoj produkt Studio Photo, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.04.2021

CVE

CVE-2021-31433, CVE-2021-31434, CVE-2021-31435, CVE-2021-31436, CVE-2021-31437, CVE-2021-31438

Zasiahnuté systémy

Foxit Studio Photo vo verzii staršej ako 3.6.6.934

Následky

Vykonanie škodlivého kódu a 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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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/200756
https://www.zerodayinitiative.com/advisories/ZDI-21-479/
https://www.foxitsoftware.com/support/security-bulletins.html

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

Identifikátor

EDIMAX IC-3140W produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť EDIMAX vydala bezpečnostnú aktualizáciu na svoj produkt IC-3140W, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

27.04.2021

CVE

CVE-2021-30165

Zasiahnuté systémy

EDIMAX IC-3140W devices vo verzii staršej ako 3.12

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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/200859
https://www.twcert.org.tw/tw/cp-132-4670-359c8-1.html
https://www.edimax.com/edimax/us/

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

Identifikátor

New Technology LAN Manager (NTLM) - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu NTLM od spoločnosti Microsoft. Kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, autentifikovanému útočníkovi s administrátorskými právomocami, prostredníctvom zasielania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

26.04.2021

CVE

-

Zasiahnuté systémy

NTLM vo verzii staršej ako 33.0 (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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 nastaviť domain controler podľa pokynov uvedených na webovej adrese:
https://labs.sentinelone.com/relaying-potatoes-dce-rpc-ntlm-relay-eop/

Zdroje

https://www.securityweek.com/ntlm-relay-attack-abuses-windows-rpc-protocol-vulnerability
https://labs.sentinelone.com/relaying-potatoes-dce-rpc-ntlm-relay-eop/
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-nlmp/b38c36ed-2804-4868-a9ff-8dd3182128e4
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H