BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 03. 2021 - 30. 03. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Mozilla Firefox - bezpečnostné zraniteľnosti	Vysoká	**8.8**
02.	SolarWinds Orion Platform - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	MyBB produkt - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Ovarro produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
05.	TIBCO produkty - viacero zraniteľností	Vysoká	**8.8**
06.	Linux Kernel - bezpečnostná zraniteľnosť	Vysoká	**8.4**
07.	Adobe ColdFusion - bezpečnostná zraniteľnosť	Vysoká	**7.8**
08.	Git-bug - bezpečnostná zraniteľnosť	Vysoká	**7.8**
09.	Foxit produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
10.	BOSH produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
11.	Zoom - bezpečnostná zraniteľnosť	Vysoká	**7.5**
12.	IBM Elastic Storage System - bezpečnostná zraniteľnosť	Vysoká	**7.5**
13.	OpenSSL - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
14.	Samba AD DC LDAP server - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**

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-378

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

Identifikátor

Mozilla Firefox - bezpečnostné zraniteľnosti

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.03.2021

CVE

CVE-2021-23981, CVE-2021-23982, CVE-2021-23983, CVE-2021-23984, CVE-2021-23985, CVE-2021-23986, CVE-2021-23987, CVE-2021-23988

Zasiahnuté systémy

Firefox ESR vo verzii staršej ako 78.9
Thunderbird vo verzii staršej ako 78.9
Firefox vo verzii staršej ako 87

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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 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.mozilla.org/en-US/security/advisories/mfsa2021-11/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-12/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-10/
https://exchange.xforce.ibmcloud.com/vulnerabilities/198593

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

Identifikátor

SolarWinds Orion Platform - bezpečnostná zraniteľnosť

Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na produkt Orion Platform, ktorá opravuje viacero bezpečnostných zraniteľností, z ktorých jedna je označovaná ako kritická.
Kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.03.2021

CVE

CVE-2020-35856, CVE-2021-3109

Zasiahnuté systémy

Orion Platform vo verzii staršej ako 2020.2.5

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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://thehackernews.com/2021/03/solarwinds-orion-vulnerability.html
https://documentation.solarwinds.com/en/Success_Center/orionplatform/Content/Release_Notes/Orion_Platform_2020-2-5_release_notes.htm

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

Identifikátor

MyBB produkt - viacero bezpečnostných zraniteľností

Popis

Vývojári open-source fóra MyBB vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.03.2021

CVE

CVE-2021-27889, CVE-2021-27890, CVE-2021-27946, CVE-2021-27947, CVE-2021-27948, CVE-2021-27949

Zasiahnuté systémy

MyBB vo verzii staršej ako 1.8.26

Následky

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

Odporúčania

Administrátorom 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://thehackernews.com/2021/03/critical-rce-flaw-reported-in-mybb.html
https://blog.mybb.com/2021/03/10/mybb-1-8-26-released-security-release/
https://blog.sonarsource.com/mybb-remote-code-execution-chain
https://github.com/mybb/mybb/security/advisories/GHSA-r34m-ccm8-mfhq
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

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

Identifikátor

Ovarro produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Ovarro vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.03.2021

CVE

CVE-2021-22640, CVE-2021-22642, CVE-2021-22644, CVE-2021-22646, CVE-2021-22648

Zasiahnuté systémy

TBoxLT2 všetky verzie
TBox MS-CPU32
TBox MS-CPU32-S2
TBox RM2 všetky verzie
TBox TG2 všetky verzie
TWinSoft vo verzii staršej ako 12.4 s Firmware vo verzii staršej ako 1.46

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://us-cert.cisa.gov/ics/advisories/icsa-21-054-04
https://exchange.xforce.ibmcloud.com/vulnerabilities/198614

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

Identifikátor

TIBCO produkty - viacero zraniteľností

Popis

Spoločnosť TIBCO vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.03.2021

CVE

CVE-2021-28817, CVE-2021-28818, CVE-2021-28819, CVE-2021-28820, CVE-2021-28821, CVE-2021-28822, CVE-2021-28823, CVE-2021-28824

Zasiahnuté systémy

TIBCO ActiveSpaces - Community Edition vo verzii staršej ako 4.6.0
TIBCO ActiveSpaces - Developer Edition vo verzii staršej ako 4.6.0
TIBCO ActiveSpaces - Enterprise Edition vo verzii staršej ako 4.6.0
TIBCO eFTL - Community Edition vo verzii staršej ako 6.6.0
TIBCO eFTL - Developer Edition vo verzii staršej ako 6.6.0
TIBCO eFTL - Enterprise Edition vo verzii staršej ako 6.6.0
TIBCO Enterprise Message Service vo verzii staršej ako 8.6.0
TIBCO Enterprise Message Service - Community Edition vo verzii staršej ako 8.6.0
TIBCO Enterprise Message Service - Developer Edition vo verzii staršej ako 8.6.0

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.

Zdroje
https://www.tibco.com/support/advisories/2021/03/tibco-security-advisory-march-23-2021-tibco-activespaces-2021-28824
https://exchange.xforce.ibmcloud.com/vulnerabilities/198668
https://exchange.xforce.ibmcloud.com/vulnerabilities/198670
https://exchange.xforce.ibmcloud.com/vulnerabilities/198670
https://exchange.xforce.ibmcloud.com/vulnerabilities/198671
https://exchange.xforce.ibmcloud.com/vulnerabilities/198685
https://exchange.xforce.ibmcloud.com/vulnerabilities/198686
https://exchange.xforce.ibmcloud.com/vulnerabilities/198687
https://exchange.xforce.ibmcloud.com/vulnerabilities/198688
https://exchange.xforce.ibmcloud.com/vulnerabilities/198689

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

Identifikátor

Linux Kernel - bezpečnostná zraniteľnosť

Popis

Vývojári Linux Kernel vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného programu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.03.2021

CVE

CVE-2021-3444

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako 5.4.101
Linux Kernel vo verzii staršej ako 5.10.19
Linux Kernel vo verzii staršej ako 5.11.2

Následky

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

Odporúčania

Administrátorom 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/198601
https://seclists.org/oss-sec/2021/q1/259
https://www.kernel.org/

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

Identifikátor

Adobe ColdFusion - bezpečnostná zraniteľnosť

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt ColdFusion, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného dokumentu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.03.2021

CVE

CVE-2021-21087

Zasiahnuté systémy

Adobe ColdFusion 2016 vo verzii staršej ako Update 17
Adobe ColdFusion 2018 vo verzii staršej ako Update 11
Adobe ColdFusion 2021 vo verzii staršej ako Update 1

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.
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://threatpost.com/adobe-critical-coldfusion-flaw-update/164946/
https://www.securityweek.com/adobe-patches-critical-coldfusion-security-flaw
https://www.bleepingcomputer.com/news/security/critical-code-execution-vulnerability-fixed-in-adobe-coldfusion/
https://www.cisecurity.org/advisory/a-vulnerability-in-adobe-coldfusion-could-allow-for-arbitrary-code-execution/

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

Identifikátor

Git-bug - bezpečnostná zraniteľnosť

Popis

Vývojári bug trackera Git-bug vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
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

21.03.2021

CVE

CVE-2021-28955

Zasiahnuté systémy

git-bug vo verzii staršej ako 0.7.2

Následky

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

Odporúčania

Administrátorom 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 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/198513
https://github.com/MichaelMure/git-bug/security/advisories/GHSA-m898-h4pm-pqfr

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

Identifikátor

Foxit produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Foxit vydala bezpečnostné aktualizácie na produkty Reader a PhantomPDF, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia 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

22.03.2021

CVE

CVE-2021-27267, CVE-2021-27268, CVE-2021-27269, CVE-2021-27270, CVE-2021-27271

Zasiahnuté systémy

Foxit Reader 10.1.3
Foxit PhantomPDF 10.1.3

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.
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/198544
https://exchange.xforce.ibmcloud.com/vulnerabilities/198545
https://exchange.xforce.ibmcloud.com/vulnerabilities/198546
https://exchange.xforce.ibmcloud.com/vulnerabilities/198547
https://exchange.xforce.ibmcloud.com/vulnerabilities/198549
https://www.foxitsoftware.com/support/security-bulletins.html

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

Identifikátor

BOSH produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť BOSH vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného DLL vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.03.2021

CVE

CVE-2020-6771, CVE-2020-6785, CVE-2020-6786, CVE-2020-6787, CVE-2020-6788, CVE-2020-6789, CVE-2020-6790

Zasiahnuté systémy

Bosch BVMS vo verzii staršej ako 9.0.0
Bosch BVMS vo verzii staršej ako 10.0.2
Bosch BVMS vo verzii staršej ako 10.1.1
Bosch BVMS Viewer vo verzii staršej ako 9.0.0
Bosch BVMS Viewer vo verzii staršej ako 10.0.2
Bosch BVMS Viewer vo verzii staršej ako 10.1.1
Bosch Configuration Manager vo verzii staršej ako 7.21.0078 (vrátane)
Bosch DIVAR IP 7000 R2 s konfiguráciou ‘using vulnerable BVMS version’
Bosch DIVAR IP all-in-one 5000 s konfiguráciou ‘using vulnerable BVMS version’
Bosch DIVAR IP all-in-one 7000 s konfiguráciou ‘using vulnerable BVMS version’
Bosch IP Helper vo verzii staršej ako 1.00.0008 (vrátane)
Bosch Monitor Wall vo verzii staršej ako 10.00.0164 (vrátane)
Bosch Video Client vo verzii staršej ako 1.7.6.079 (vrátane)
Bosch Video Recording Manager vo verzii staršej ako 3.71 (vrátane)
Bosch Video Recording Manager vo verzii staršej ako 3.81.0064 (vrátane)
Bosch Video Recording Manager vo verzii staršej ako 3.82.0055 (vrátane)
Bosch Video Streaming Gateway vo verzii staršej ako 6.45.10 (vrátane)

Následky

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

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

Zdroje
https://psirt.bosch.com/security-advisories/bosch-sa-835563-bt.html

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

Identifikátor

Zoom - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Zoom.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

18.03.2021

CVE

CVE-2021-28133

Zasiahnuté systémy

Zoom vo verzii staršej ako 5.4.3 (54779.1115) (vrátane)
Zoom vo verzii staršej ako 5.5.4 (13142.0301) (vrátane)

Následky

Neoprávnený prístup k citlivým údajom

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://thehackernews.com/2021/03/new-zoom-screen-sharing-bug-lets-other.html
https://threatpost.com/zoom-glitch-leaks-data/164876/
https://seclists.org/fulldisclosure/2021/Mar/48
https://exchange.xforce.ibmcloud.com/vulnerabilities/198406

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

Identifikátor

IBM Elastic Storage System - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoj produkt Elastic Storage System, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených UDP požiadaviek spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

23.03.2021

CVE

CVE-2020-5015

Zasiahnuté systémy

IBM Elastic Storage System vo verzii staršej ako V6.1.0.0
IBM Elastic Storage System vo verzii staršej ako V6.0.2.0
IBM Elastic Storage Server vo verzii staršej ako V5.3.7

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.ibm.com/support/pages/node/6434155
https://www.ibm.com/support/pages/node/6434737
https://exchange.xforce.ibmcloud.com/vulnerabilities/193486

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

Identifikátor

OpenSSL - dve bezpečnostné zraniteľnosti

Popis

Vývojári knižnice OpenSSL vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej ClientHello správy spôsobiť zneprístupnenie služby.
Na jednu zo zraniteľností je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

25.03.2021

CVE

CVE-2021-3449, CVE-2021-3450

Zasiahnuté systémy

OpenSSL vo verzii staršej ako 1.1.1k

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.bleepingcomputer.com/news/security/openssl-fixes-severe-dos-certificate-validation-vulnerabilities/
https://thehackernews.com/2021/03/openssl-releases-patches-for-2-high.html
https://github.com/terorie/cve-2021-3449
https://www.openssl.org/news/secadv/20210325.txt
https://github.com/openssl/openssl/commit/468d9d556409a53da2c5d16961f9531dd10a6e1b
https://access.redhat.com/security/cve/CVE-2021-3449
https://exchange.xforce.ibmcloud.com/vulnerabilities/198752
https://exchange.xforce.ibmcloud.com/vulnerabilities/198754

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

Identifikátor

Samba AD DC LDAP server - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Samba vydala bezpečnostné aktualizácie na produkt Samba AD DC LDAP server, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

24.03.2021

CVE

CVE-2020-27840, CVE-2021-20277

Zasiahnuté systémy

Samba vo verzii staršej ako 4.14.2
Samba vo verzii staršej ako 4.13.7
Samba vo verzii staršej ako 4.12.14

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.samba.org/samba/security/CVE-2020-27840.html
https://www.samba.org/samba/security/CVE-2021-20277.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/198777