



OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	PHP viacero zraniteľností	Vysoká	8.8
02.	Rockwell Automation Arena Simulation Software	Vysoká	8.8
03.	NVIDIA GPU Display Driver zraniteľnosti	Vysoká	8.8
04.	VMware ESXi, Workstation a Fusion zraniteľnosti	Vysoká	8.5
05.	Advantech WebAccess HMI Designer zraniteľnosť	Vysoká	7.8
06.	Pallets Werkzeug zraniteľnosť	Vysoká	7.5
07.	GnuCOBOL zraniteľnosti	Vysoká	7.3
08.	VirusTotal YARA zraniteľnosť	Stredná	6.5



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

PHP viacero zraniteľností

Popis

Vývojári skriptovacieho jazyka PHP vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.08.2019

CVE

CVE-2019-11041, CVE-2019-11042

Zasiiahnuté systémy

PHP verzie staršie ako 7.3.8

PHP verzie staršie ako 7.2.21

PHP verzie staršie ako 7.1.31

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://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-arbitrary-code-execution-2019-077/>

<https://bugs.php.net/bug.php?id=78222>

<https://bugs.php.net/bug.php?id=78256>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Rockwell Automation Arena Simulation Software

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností v simulátore Arena Simulation Software.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.08.2019

CVE

CVE-2019-13510, CVE-2019-13511

Zasiahnuté systémy

Rockwell Automation Arena Simulation Software for Manufacturing, Cat. 9502-Ax, verzie staršie ako 16.00.01

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a aplikovať firewallové pravidlá.

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

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://www.us-cert.gov/ics/advisories/icsa-19-213-05>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

NVIDIA GPU Display Driver zraniteľnosti

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na svoje ovládače pre grafické karty GeForce, Quadro, NVS a Tesla, ktoré opravujú viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.08.2019

CVE

CVE-2019-5683, CVE-2019-5684, CVE-2019-5685, CVE-2019-5686, CVE-2019-5687

Zasiiahnuté systémy

NVIDIA GeForce R430 verzie staršie ako 431.60
NVIDIA Quadro, NVS R430 verzie staršie ako 431.70
NVIDIA Quadro, NVS R418 verzie staršie ako 426.00
NVIDIA Quadro, NVS R390 verzie staršie ako 392.56
NVIDIA Quadro, NVS R400 všetky verzie
NVIDIA Tesla R418 všetky verzie

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiiahnutým zariadeniam 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.

Zdrojehttps://nvidia.custhelp.com/app/answers/detail/a_id/4841<https://www.bleepingcomputer.com/news/security/nvidia-patches-high-severity-flaws-in-windows-gpu-display-driver/>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

VMware ESXi, Workstation a Fusion zraniteľnosti

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje produkty ESXi, Workstation a Fusion, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov, podmienená nainštalovaným driverom NVIDIA graphics na hostoch a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.08.2019

CVE

CVE-2019-5521, CVE-2019-5684

Zasiahnuté systémy

VMware ESXi verzie staršie ako 650-201903001
VMware ESXi verzie staršie ako 670-201904101-SG
VMware Workstation verzie staršie ako 14.1.6
VMware Workstation verzie staršie ako 15.0.3
VMware Fusion verzie staršie ako 10.1.6
VMware Fusion verzie staršie ako 11.0.3

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam 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://www.vmware.com/security/advisories/VMSA-2019-0012.html>
https://nvidia.custhelp.com/app/answers/detail/a_id/4841



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Advantech WebAccess HMI Designer zraniteľnosť

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na svoj produkt WebAccess HMI Designer, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.08.2019

CVE

CVE-2019-10961

Zasiahnuté systémy

Advantech WebAccess HMI Designer, a Human Machine Interface (HMI) verzie staršie ako 2.1.9.31

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://www.us-cert.gov/ics/advisories/icsa-19-213-01>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Pallets Werkzeug zraniteľnosť

Popis

Vývojári knižnice Pallets Werkzeug vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii SharedDataMiddleware.

Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

02.08.2019

CVE

CVE-2019-14322

Zasiiahnuté systémy

Pallets Werkzeug verzie staršie ako 0.15.5

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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://tools.cisco.com/security/center/viewAlert.x?alertId=60517>

<https://palletsprojects.com/blog/werkzeug-0-15-5-released/>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.3
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

GnuCOBOL zraniteľnosti

Popis

Bezpečnostní výskumníci zveřejnili informace o bezpečnostní zranitelnosti v kompilátore programovacího jazyka GnuCOBOL.

Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi pomocou špeciálne vytvoreného COBOL zdrojového kódu spôsobiť pretečenie zásobníka a vykonať škodlivý kód alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.08.2019

CVE

CVE-2019-14468, CVE-2019-14486

Zasiahnuté systémy

GnuCOBOL

Následky

Vykonanie škodlivého kódu

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

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/164698>

<https://exchange.xforce.ibmcloud.com/vulnerabilities/164699>



Dôležitosť	<input type="checkbox"/> Nízka	<input checked="" type="checkbox"/> Stredná	<input type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 6.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

VirusTotal YARA zraniteľnosť

Popis

Spoločnosť VirusTotal vydala bezpečnostnú aktualizáciu na svoj nástroj pre identifikáciu a klasifikáciu malware, ktorá upravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru spôsobiť znepřístupnenie služby. Proof-of-concept (PoC) kód je verejne dostupný.

Dátum prvého zverejnenia varovania

02.05.2019

CVE

CVE-2019-5020

Zasiiahnuté systémy

VirusTotal YARA verzie staršie ako 3.10.0

Následky

Znepřístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

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

Zdroje

<https://tools.cisco.com/security/center/viewAlert.x?alertId=60550>

<https://github.com/virustotal/yara/releases/tag/v3.10.0>