



## OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	mySCADA myPRO produkt - bezpečnostná zraniteľnosť	Vysoká	8.8
02.	Google Chrome - bezpečnostná zraniteľnosť	Vysoká	8.8
03.	Yokogawa CENTUM a Exaopc produkty - viacero bezpečnostných zraniteľností	Vysoká	8.6
04.	Razer Synapse produkt - bezpečnostná zraniteľnosť	Vysoká	7.8
05.	Jupyter Server - bezpečnostná zraniteľnosť	Vysoká	7.5
06.	Okta Advanced Server Access Client - bezpečnostná zraniteľnosť	Vysoká	7.5



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(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

mySCADA myPRO produkt - bezpečnostná zraniteľnosť

#### Popis

Spoločnosť mySCADA vydala bezpečnostnú aktualizáciu na produkt myPRO, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

#### Dátum prvého zverejnenia varovania

25.03.2022

#### CVE

CVE-2022-0999

#### Zasiiahnuté systémy

myPRO vo verzii staršej ako 8.26.0

#### 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.

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

#### Zdroje

<https://us-cert.cisa.gov/ics/advisories/icsa-22-083-02>



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(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

Google Chrome - bezpečnostná zraniteľnosť

#### Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na produkt Chrome, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorenej webovej stránky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

#### Dátum prvého zverejnenia varovania

25.03.2022

#### CVE

CVE-2022-1096

#### Zasiahnuté systémy

Google Chrome vo verzii staršej ako 99.0.4844.84

#### 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.

#### Zdroje

[https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop\\_25.html](https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_25.html)

<https://www.cisecurity.org/advisory/a-vulnerability-in-google-chrome-could-allow-for-arbitrary-code-execution-2022-040>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.6
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

**Identifikátor**

Yokogawa CENTUM a Exaopc produkty - viacero bezpečnostných zraniteľností

**Popis**

Spoločnosť Yokogawa vydala bezpečnostnú aktualizáciu na produkty CENTUM a Exaopc, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených paketov, eskalovať svoje privilégia a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

**Dátum prvého zverejnenia varovania**

25.03.2022

**CVE**

CVE-2022-21177, CVE-2022-21194, CVE-2022-21808, CVE-2022-22141, CVE-2022-22145, CVE-2022-22148, CVE-2022-22151, CVE-2022-22729, CVE-2022-23401, CVE-2022-23402

**Zasiahnuté systémy**

CENTUM VP vo verzii staršej ako R6.09.00

CENTUM CS 3000 výrobcu odporúča migrovať na najnovšiu verziu CENTUM VP

Exaopc vo verzii staršej ako R3.80.00

**Následky**

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

Eskalácia privilégii

**Odporúčania**

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Po odstránení zraniteľností, ktoré mohli spôsobiť lokálne 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 administratívne 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-22-083-01>



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(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

Razer Synapse produkt - bezpečnostná zraniteľnosť

#### Popis

Spoločnosť Razer vydala bezpečnostnú aktualizáciu na produkt Synapse, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvoreného súboru, eskalovať svoje privilégia a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

#### Dátum prvého zverejnenia varovania

23.03.2022

#### CVE

CVE-2021-44226

#### Zasiahnuté systémy

Razer Synapse vo verzii staršej ako 3.7.0228.022817

#### 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 lokálne 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 administratívnejmu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

#### Zdroje

<https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-058.txt>

<https://www2.razer.com/eu-en/synapse-3>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44226>

<https://exchange.xforce.ibmcloud.com/vulnerabilities/222454>



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(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

Jupyter Server - bezpečnostná zraniteľnosť

#### Popis

Vývojári nástroja Jupyter Server vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

#### Dátum prvého zverejnenia varovania

23.03.2022

#### CVE

CVE-2022-24757

#### Zasiiahnuté systémy

Jupyter Server vo verzii staršej ako 1.15.4

#### 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://github.com/jupyter-server/jupyter\\_server/security/advisories/GHSA-p737-p57g-4cpr](https://github.com/jupyter-server/jupyter_server/security/advisories/GHSA-p737-p57g-4cpr)

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24757>

<https://exchange.xforce.ibmcloud.com/vulnerabilities/222427>



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(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

**Identifikátor**

Okta Advanced Server Access Client - bezpečnostná zraniteľnosť

**Popis**

Vývojári nástroja Okta Advanced Server Access Client vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

**Dátum prvého zverejnenia varovania**

21.03.2022

**CVE**

CVE-2022-1030

**Zasiahnuté systémy**

Okta Advanced Server Access Client pre Linux a macOS vo verzii staršej ako 1.58.0

**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.

**Zdroje**<https://trust.okta.com/security-advisories/okta-advanced-server-access-client-cve-2022-1030/><http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1030><https://exchange.xforce.ibmcloud.com/vulnerabilities/222495>