# BEZPEČNOSTNÝ BULLETIN

Týždeň 05. 05. 2022 - 11. 05. 2022

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Č. | Identifikátor | Dôležitosť | CVSS Skóre |
|---|---|---|---|
| **01.** | Kingsoft WPS Office - bezpečnostná zraniteľnosť | Vysoká | **8.8** |
| **02.** | QNAP produkty - viacero bezpečnostných zraniteľností | Vysoká | **8.8** |
| **03.** | rsyslog nástroj - bezpečnostná zraniteľnosť | Vysoká | **8.1** |
| **04.** | Johnson Controls Metasys ADS/ADX/OAS produkty - bezpečnostná zraniteľnosť | Vysoká | **8.0** |
| **05.** | F5 BIG-IP ASM, Advanced WAF, APM - bezpečnostná zraniteľnosť | 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:
01794/2022/SK-CERT-751

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

## Identifikátor

Kingsoft WPS Office - bezpečnostná zraniteľnosť

## Popis

Vývojári kancelárskeho balíka WPS Office vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených XLS súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

09.05.2022

## CVE

CVE-2021-40399

## Zasiahnuté systémy

Kingsoft WPS Office vo verzii staršej ako 11.8.2.11542

## 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 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.

## Zdroje

https://talosintelligence.com/vulnerability_reports/TALOS-2021-1412
https://www.wps.com/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40399
https://exchange.xforce.ibmcloud.com/vulnerabilities/225992

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

## Identifikátor

QNAP produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť QNAP vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch QTS, QuTS hero, QuTScloud a QNAP NAS využívajúcich funkcionalitu Video Station a Photo Station.

Najzávažnejšia zraniteľnosť sa nachádza v produktoch QTS, QuTS hero a QuTScloud, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

06.05.2022

## CVE

CVE-2021-44051, CVE-2021-44052, CVE-2021-44053, CVE-2021-44054, CVE-2021-44055, CVE-2021-44056, CVE-2021-44057

## Zasiahnuté systémy

Video Station vo verzii staršej ako 5.5.9
Video Station vo verzii staršej ako 5.3.13
Video Station vo verzii staršej ako 5.1.8
Photo Station vo verzii staršej ako 6.0.20 (2022/02/15)
Photo Station vo verzii staršej ako 5.7.16 (2022/02/11)
Photo Station vo verzii staršej ako 5.4.13 (2022/02/11)
QTS vo verzii staršej ako 5.0.0.1986 build 20220324
QTS vo verzii staršej ako 4.5.4.1991 build 20220329
QTS vo verzii staršej ako 4.3.6.1965 build 20220302
QTS vo verzii staršej ako 4.3.4.1976 build 20220303
QTS vo verzii staršej ako 4.3.3.1945 build 20220303
QTS vo verzii staršej ako 4.2.6 build 20220304
QuTS hero h5.0.0.1986 vo verzii staršej ako build 20220324
QuTS hero h4.5.4.1971 vo verzii staršej ako build 20220310
QuTScloud vo verzii staršej ako c5.0.1.1998

## Následky

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

| **Odporúčania** |
| --- |
| Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.<br>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.qnap.com/en/security-advisory/qsa-22-14<br>https://www.qnap.com/en/security-advisory/qsa-22-15<br>https://www.qnap.com/en/security-advisory/qsa-22-16<br>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44051<br>https://exchange.xforce.ibmcloud.com/vulnerabilities/225864 |

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

## Identifikátor

rsyslog nástroj - bezpečnostná zraniteľnosť

## Popis

Vývojári nástroja rsyslog vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v komponente TCP syslog server (receiver).
Bezpečnostná zraniteľnosť v spočíva v nedostatočnom overovaní prijatých požiadaviek a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

05.05.2022

## CVE

CVE-2022-24903

## Zasiahnuté systémy

rsyslog vo verzii staršej ako 8.2204.1

## 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.

## Zdroje

https://seclists.org/oss-sec/2022/q2/85
https://github.com/rsyslog/rsyslog/security/advisories/GHSA-ggw7-xr6h-mmr8
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24903
https://exchange.xforce.ibmcloud.com/vulnerabilities/225843

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 8.0** |
| **Klasifikácia** | ☒ **Neutajované / TLP(CLEAR)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Johnson Controls Metasys ADS/ADX/OAS produkty - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na produkty Metasys ADS/ADX/OAS Servers, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a autentifikovaný útočík v rovnakom sieťovom segmente by ju mohol zneužiť na zablokovanie prístupu a získanie kontroly nad používateľskými kontami ostatných používateľov systému.

## Dátum prvého zverejnenia varovania

05.05.2022

## CVE

CVE-2022-21934

## Zasiahnuté systémy

Metasys ADS/ADX/OAS Servers vo verzii staršej ako 10.1.5
Metasys ADS/ADX/OAS Servers vo verzii staršej ako 11.0.2

## Následky

Zneprístupnenie služby
Eskalácia privilégií

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

## Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-125-01
https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2022/jci-psa-2022-09.pdf?la=en&hash=CDBC2D715E982A79F3A11C86819CF4766F047274

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

## Identifikátor

F5 BIG-IP ASM, Advanced WAF, APM - bezpečnostná zraniteľnosť

## Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na produkty BIG-IP ASM, Advanced WAF a APM, ktorá opravuje bezpečnostnú zraniteľnosť.
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

04.05.2022

## CVE

CVE-2022-26890

## Zasiahnuté systémy

F5 BIG-IP ASM, Advanced WAF, APM vo verzii staršej ako 17.0.0
F5 BIG-IP ASM, Advanced WAF, APM vo verzii staršej ako 16.1.2.1
F5 BIG-IP ASM, Advanced WAF, APM vo verzii staršej ako 15.1.5
F5 BIG-IP ASM, Advanced WAF, APM vo verzii staršej ako 14.1.4.6
F5 BIG-IP ASM, Advanced WAF, APM vo verzii staršej ako 13.1.5

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://support.f5.com/csp/article/K03442392
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26890
https://exchange.xforce.ibmcloud.com/vulnerabilities/225745