BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 12. 2022 - 03. 01. 2023

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:
01794/2022/SK-CERT-979

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

Identifikátor

D-Link DIR-825/EE - viacero bezpečnostných zraniteľností

Popis

Spoločnosť D-Link vydala bezpečnostnú aktualizáciu na svoj router DIR-825/EE, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.12.2022

CVE

CVE-2022-43642, CVE-2022-43643, CVE-2022-43644, CVE-2022-43645, CVE-2022-43646, CVE-2022-43647

Zasiahnuté systémy

DIR-825/EE s firmvérom vo verzii staršej ako v1.0.10_Beta_Hotfix

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.
Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10319
https://www.zerodayinitiative.com/advisories/ZDI-22-1706/
https://www.zerodayinitiative.com/advisories/ZDI-22-1705/
https://www.zerodayinitiative.com/advisories/ZDI-22-1704/
https://www.zerodayinitiative.com/advisories/ZDI-22-1703/
https://www.zerodayinitiative.com/advisories/ZDI-22-1702/
https://www.zerodayinitiative.com/advisories/ZDI-22-1701/

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-979

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

Identifikátor

X.Org Server - viacero bezpečnostných zraniteľností

Popis

Vývojári serveru X.Org vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom znovupoužitia uvoľnenej pamäte vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.12.2022

CVE

CVE-2022-4283, CVE-2022-46283, CVE-2022-46340, CVE-2022-46341, CVE-2022-46342, CVE-2022-46343, CVE-2022-46344

Zasiahnuté systémy

xorg-server vo verzii staršej ako 21.1.5

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.zerodayinitiative.com/advisories/ZDI-22-1700/
https://lists.x.org/archives/xorg-announce/2022-December/003302.html

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

Identifikátor

Fuji Electric - viaceo bezpečnostných zraniteľností

Popis

Spoločnosť Fuji Electric 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 zneužitia out-of-bounds zápisu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.12.2022

CVE

CVE-2022-41645, CVE-2022-43448, CVE-2022-46360, CVE-2022-47317, CVE-2022-47908

Zasiahnuté systémy

Fuji Electric V-SFT vo verzii staršej ako 6.1.8.0
Fuji Electric TELLUS vo verzii staršej ako 4.0.15.0

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.
Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.
Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

http://jvn.jp/en/vu/JVNVU92811888/index.html
http://jvn.jp/en/vu/JVNVU90679513/index.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/243169