BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 09. 2022 - 20. 09. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

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

Identifikátor

Siemens - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom čiastočného narušenia dôvernosti a integrity, a úplného narušenia dostupnosti systému.

Dátum prvého zverejnenia varovania

13.09.2022

CVE

CVE-2016-0701, CVE-2020-12762, CVE-2020-28168, CVE-2020-28500, CVE-2020-7793, CVE-2021-23337, CVE-2021-23839, CVE-2021-23841, CVE-2021-25217, CVE-2021-25220, CVE-2021-3749, CVE-2021-4160, CVE-2022-0155, CVE-2022-0235, CVE-2022-0396, CVE-2022-37011, CVE-2022-38466, CVE-2022-39137, CVE-2022-39138, CVE-2022-39139, CVE-2022-39140, CVE-2022-39141, CVE-2022-39142, CVE-2022-39143, CVE-2022-39144, CVE-2022-39145, CVE-2022-39146, CVE-2022-39147, CVE-2022-39148, CVE-2022-39149, CVE-2022-39150, CVE-2022-39151, CVE-2022-39152, CVE-2022-39153, CVE-2022-39154, CVE-2022-39155, CVE-2022-39156

Zasiahnuté systémy

SINEC INS vo verzii staršej ako V1.0 SP2
CoreShield One-Way vo verzii staršej ako V2.2
Parasolid V33.1 vo verzii staršej ako V33.1.263
Parasolid V34.0 vo verzii staršej ako V34.0.252
Parasolid V34.1 vo verzii staršej ako V34.1.242
Parasolid V35.0 vo verzii staršej ako V35.0.164
Simcenter Femap V2022.1 vo verzii staršej ako V2022.1.3
Simcenter Femap V2022.2 vo verzii staršej ako V2022.2.2
Mendix SAML Module vo verzii staršej ako V3.3.1

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://cert-portal.siemens.com/productcert/html/ssa-518824.html
https://cert-portal.siemens.com/productcert/html/ssa-589975.html
https://cert-portal.siemens.com/productcert/html/ssa-637483.html
https://cert-portal.siemens.com/productcert/html/ssa-638652.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

HP EliteBook - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktovej rady HP EliteBook. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.09.2022

CVE

CVE-2022-23930, CVE-2022-31640, CVE-2022-31641, CVE-2022-31644, CVE-2022-31645, CVE-2022-31646

Zasiahnuté systémy

HP EliteBook s BIOS vo verzii staršej ako 8.9.2022 (vrátane)

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nebola vydaná bezpečnostná záplata, administrátorom preto odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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://binarly.io/posts/Binarly_Finds_Six_High_Severity_Firmware_Vulnerabilities_in_HP_Enterprise_Devices/index.html
https://www.bleepingcomputer.com/news/security/firmware-bugs-in-many-hp-computer-models-left-unfixed-for-over-a-year/
https://nvd.nist.gov/vuln/detail/CVE-2022-23930

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

Identifikátor

Microsoft Windows Common Log File System - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj ovládač Windows Common Log File System, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

16.09.2022

CVE

CVE-2022-37969

Zasiahnuté systémy

Microsoft Windows Common Log File System vo verzii staršej ako September 2022 Microsoft security update

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému.

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://nvd.nist.gov/vuln/detail/CVE-2022-37969

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

NETGEAR - bezpečnostná zraniteľnosť

Popis

Spoločnosť NETGEAR vydala bezpečnostnú aktualizáciu na svoje portfólio routerov a WiFi systémov, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov spôsobiť úplné narušenie dôvernosti a integrity a čiastočné narušenie dostupnosti systému.

Dátum prvého zverejnenia varovania

08.09.2022

CVE

CVE-2022-40619, CVE-2022-40620

Zasiahnuté systémy

RBR20 vo verzii staršej ako 2.7.2.26
RBR50 vo verzii staršej ako 2.7.4.26
RBS20 vo verzii staršej ako 2.7.2.26
RBS50 vo verzii staršej ako 2.7.4.26
R6230 vo verzii staršej ako 1.1.0.112
R6260 vo verzii staršej ako 1.1.0.88
R7000 vo verzii staršej ako 1.0.11.134
R8900 vo verzii staršej ako 1.0.5.42
R9000 vo verzii staršej ako 1.0.5.42
RAX120 vo verzii staršej ako 1.2.8.40
RAX120v2 vo verzii staršej ako 1.2.8.40
XR300 vo verzii staršej ako 1.0.3.72

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

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://kb.netgear.com/000065132/Security-Advisory-for-Vulnerabilities-in-FunJSQ-on-Some-Routers-and-Orbi-WiFi-Systems-PSV-2022-0117

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

Identifikátor

BackupBuddy WordPress plugin - bezpečnostná zraniteľnosť

Popis

Vývojári WordPress pluginu BackupBuddy vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

07.09.2022

CVE

CVE-2022-31474

Zasiahnuté systémy

BackupBuddy vo verzii staršej ako 8.7.5

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú daný plugin v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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://www.wordfence.com/blog/2022/09/psa-nearly-5-million-attacks-blocked-targeting-0-day-in-backupbuddy-plugin/