BEZPEČNOSTNÝ BULLETIN

Týždeň 29. 09. 2021 - 05. 10. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Salesforce Developer Experience Command Line Interface - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	3xLogic Infinias Access Control - bezpečnostná zraniteľnosť	Vysoká	**8.1**
03.	HX CMSimple_HX - bezpečnostná zraniteľnosť	Vysoká	**8.1**
04.	BIQS IT Biqs-drive - 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:
01439/2020/SK-CERT-574

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

Identifikátor

Salesforce Developer Experience Command Line Interface - bezpečnostná zraniteľnosť

Popis

Spoločnosť Salesforce vydala bezpečnostnú aktualizáciu na svoj produkt DX (Developer Experience), ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť umožňuje vzdialenému autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.10.2021

CVE

-

Zasiahnuté systémy

Salesforce DX command line interface

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://help.salesforce.com/s/articleView?id=000363271&type=1
http://www.kb.cert.org/vuls/id/883754
https://exchange.xforce.ibmcloud.com/vulnerabilities/210639

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

Identifikátor

3xLogic Infinias Access Control - bezpečnostná zraniteľnosť

Popis

Spoločnosť 3xLogic vydala bezpečnostnú aktualizáciu na produkt Infinias Access Control, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

01.10.2021

CVE

CVE-2021-41847

Zasiahnuté systémy

3xLogic Infinias Access Control vo verzii staršej ako 6.7.10708.0 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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://grant-rose.com/infinias-access-control-vulnerability/
https://www.3xlogic.com/infinias-access-control
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41847
https://exchange.xforce.ibmcloud.com/vulnerabilities/210529

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

Identifikátor

HX CMSimple_HX - bezpečnostná zraniteľnosť

Popis

Spoločnosť HX vydala bezpečnostnú aktualizáciu na produkt CMSimple_HX, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť 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

01.10.2021

CVE

-

Zasiahnuté systémy

HX CMSimple_XH vo verzii staršej ako 1.7.4 (vrátane)

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom a používateľom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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.cmsimple-xh.org/?Legal-Notice
https://packetstormsecurity.com/files/164349
https://www.exploit-db.com/exploits/50367
https://exchange.xforce.ibmcloud.com/vulnerabilities/210516

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

Identifikátor

BIQS IT Biqs-drive - bezpečnostná zraniteľnosť

Popis

Spoločnosť BIQS IT vydala bezpečnostnú aktualizáciu na produkt Biqs-drive, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

04.10.2021

CVE

CVE-2021-39433

Zasiahnuté systémy

BIQS IT Biqs-drive vo verzii staršej ako 1.83 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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/PinkDraconian/CVE-2021-39433/blob/main/README.md
https://biqs-drive.be/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39433
https://exchange.xforce.ibmcloud.com/vulnerabilities/210602

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:
01439/2020/SK-CERT-574