



OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Polkit produkt - bezpečnostná zraniteľnosť	Vysoká	8.4
02.	Microsoft Edge - bezpečnostná zraniteľnosť	Vysoká	8.2
03.	Realtek RTL8710C WiFi modul - dve bezpečnostné zraniteľnosti	Vysoká	8.0
04.	OpenText Brava - viacero bezpečnostných zraniteľností	Vysoká	7.8
05.	Webex player - viacero bezpečnostných zraniteľností	Vysoká	7.8
06.	Backstage produkt- dve bezpečnostné zraniteľnosti	Vysoká	7.5



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.4
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Polkit produkt - bezpečnostná zraniteľnosť

Popis

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

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, eskalovať svoje privilégia a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.06.2021

CVE

CVE-2021-3560

Zasiahnuté systémy

Polkit vo verzii staršej ako 0.119

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Administrátorom odporúčame limitovať prístup k administratívnejmu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

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://exchange.xforce.ibmcloud.com/vulnerabilities/202979>

<https://seclists.org/oss-sec/2021/q2/180>

<https://gitlab.freedesktop.org/polkit/polkit/-/commit/a04d13a>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.2
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Microsoft Edge - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj produkt Edge, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

04.06.2021

CVE

CVE-2021-33741

Zasiahnuté systémy

Microsoft Edge vo verzii staršej ako 91.0.864.41

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-33741>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.0
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Realtek RTL8710C WiFi modul - dve bezpečnostné zraniteľnosti

Popis

Vývojári WiFi modulu Realtek RTL8710C vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza v rovnakom sieťovom segmente, prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.06.2021

CVE

CVE-2020-27301, CVE-2020-27302

Zasiahnuté systémy

Realtek RTL8710C s firmware vo verzii staršej ako 11/01/2021

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Administrátorom odporúčame limitovať prístup k administratívnejmu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

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.vdoo.com/blog/realtek-wifi-vulnerabilities-zero-day>

<https://thehackernews.com/2021/06/researchers-warn-of-critical-bugs.html>

https://github.com/ambiot/ambz2_sdk/tree/master/project/realtek_amebaz2_v0_example/GCC-RELEASE



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

OpenText Brava - viacero bezpečnostných zraniteľností

Popis

Vývojári programu OpenText Brava vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.06.2021

CVE

CVE-2021-31490, CVE-2021-31491, CVE-2021-31492, CVE-2021-31493, CVE-2021-31494, CVE-2021-31495, CVE-2021-31496, CVE-2021-31497, CVE-2021-31499, CVE-2021-31502

Zasiahnuté systémy

OpenText Brava vo verzii staršej ako 6.6.4.114

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Administrátorom odporúčame limitovať prístup k administratívnejmu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje<https://exchange.xforce.ibmcloud.com/vulnerabilities/202989><https://www.opentext.com/><https://www.zerodayinitiative.com/advisories/ZDI-21-630/>



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

Webex player - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Webex player, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.06.2021

CVE

CVE-2021-1502, CVE-2021-1503, CVE-2021-1526, CVE-2021-1528

Zasiahnuté systémy

Webex Player vo verzii staršej ako 41.5

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Administrátorom odporúčame limitovať prístup k administratívnejmu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-player-kOf8zVT>
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-player-rCFDeVj2>
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-player-dOJ2jOJ>
<https://exchange.xforce.ibmcloud.com/vulnerabilities/202905>
<https://exchange.xforce.ibmcloud.com/vulnerabilities/202904>



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

Backstage produkt- dve bezpečnostné zraniteľnosti

Popis

Vývojári programu Backstage vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

03.06.2021

CVE

CVE-2021-32660, CVE-2021-32662

Zasiahnuté systémy

Backstage techdocs-common vo verzii staršej ako 0.6.3

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://exchange.xforce.ibmcloud.com/vulnerabilities/203049>

<https://github.com/backstage/backstage/security/advisories/GHSA-pgf8-28gg-vpr6>