



OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Lexmark Printer Software G2 Installation Package - bezpečnostná zraniteľnosť	Vysoká	8.4
02.	Advantech WebAccess HMI Designer - viacero bezpečnostných zraniteľností	Vysoká	7.8
03.	FATEK Automation WinProladder produkt - viacero bezpečnostných zraniteľností	Vysoká	7.8
04.	VMware Tools pre Windows - bezpečnostná zraniteľnosť	Vysoká	7.8
05.	Zephyr RTOS - viacero bezpečnostných zraniteľností	Vysoká	7.7
06.	ABB Wibu CodeMeter - bezpečnostná zraniteľnosť	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

Lexmark Printer Software G2 Installation Package - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Lexmark Printer Software G2 Installation Package.

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

21.06.2021

CVE

-

Zasiahnuté systémy

Lexmark Printer Software G2 Installation Package vo verzii staršej ako 1.8.0.0 (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Administrátorom odporúčame limitovať prístup k administratívne 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.lexmark.com/en_us.html

<https://exchange.xforce.ibmcloud.com/vulnerabilities/204093>

<https://threatpost.com/lexmark-printers-code-execution-zero-day/167111/>



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

Advantech WebAccess HMI Designer - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu Advantech WebAccess HMI Designer.

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

Dátum prvého zverejnenia varovania

23.06.2021

CVE

CVE-2021-33000, CVE-2021-33002, CVE-2021-33004

Zasiahnuté systémy

WebAccess HMI Designer vo verzii staršej ako 2.1.9.95 (vrátane)

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.

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).

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje<https://www.advantech.com/contact><https://us-cert.cisa.gov/ics/advisories/icsa-21-173-01>



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

FATEK Automation WinProladder produkt - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu FATEK Automation WinProladder.

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

Dátum prvého zverejnenia varovania

29.06.2021

CVE

CVE-2021-32988, CVE-2021-32990, CVE-2021-32992

Zasiahnuté systémy

FATEK Automation WinProladder vo verzii staršej ako 3.30 (vrátane)

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.

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).

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje<https://us-cert.cisa.gov/ics/advisories/icsa-21-175-01>



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

VMware Tools pre Windows - bezpečnostná zraniteľnosť

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt Tools pre Windows, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.06.2021

CVE

CVE-2021-21999

Zasiahnuté systémy

VMware Tools for Windows vo verzii staršej ako 11.2.6
VMware Remote Console for Windows vo verzii staršej ako 12.0.1
VMware App Volumes vo verzii staršej ako 4 2103
VMware App Volumes vo verzii staršej ako 2.18.10

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://www.vmware.com/security/advisories/VMSA-2021-0013.html>
<https://www.securityweek.com/vmware-patches-privilege-escalation-vulnerability-tools-windows>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.7
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Zephyr RTOS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Zephyr vydala bezpečnostnú aktualizáciu na svoj produkt Zephyr RTOS, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom pretečenia zásobníka, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.06.2021

CVE

CVE-2021-3430, CVE-2021-3431, CVE-2021-3432, CVE-2021-3433, CVE-2021-3434, CVE-2021-3435, CVE-2021-3454, CVE-2021-3455

Zasiahnuté systémy

Zephyr RTOS vo verzii staršej ako 2.6.0

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.

Zdroje

<https://www.synopsys.com/blogs/software-security/cyrc-advisory-zephyr-vulnerability/>

<https://www.bleepingcomputer.com/news/security/zephyr-rtos-fixes-bluetooth-bugs-that-may-lead-to-code-execution/>



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

ABB Wibu CodeMeter - bezpečnostná zraniteľnosť

Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na svoj produkt Wibu CodeMeter, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej HTTP požiadavky, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

21.06.2021

CVE

CVE-2021-20094

Zasiiahnuté systémy

Wibu CodeMeter vo verzii staršej ako V7.21a

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

<https://search.abb.com/library/Download.aspx?DocumentID=3ADR010770&LanguageCode=en&DocumentPartId=&Action=Launch>