BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 07. 2020 - 07. 07. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Avast/ AVG Antivirus - viacero zraniteľností	Vysoká	**8.8**
02.	Mozilla Firefox - viacero zraniteľností	Vysoká	**8.8**
03.	Microsoft Windows Codecs Library - zraniteľnosti	Vysoká	**8.8**
04.	Netgear produkty - viacero zraniteľností	Vysoká	**8.8**
05.	Cisco produkty viacero zraniteľností	Vysoká	**8.1**
06.	PHOENIX CONTACT PC Worx - zraniteľnosti	Vysoká	**7.8**
07.	Delta Electronics DOPSoft - zraniteľnosti	Vysoká	**7.8**
08.	Check Point ZoneAlarm - zraniteľnosť	Vysoká	**7.8**
09.	Mitsubishi Electric Factory Automation - viacero zraniteľností	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-171

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

Identifikátor

Avast/ AVG Antivirus - viacero zraniteľností

Popis

Spoločnosť Avast vydala bezpečnostné aktualizácie na svoje antivírusové produkty Avast a AVG, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

02.06.2020

CVE

CVE-2020-13657

Zasiahnuté systémy

Avast Free Antivirus verzie staršie ako 20.4
AVG AntiVirus Free verzie staršie ako 20.4

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://forum.avast.com/index.php?topic=234638.0
https://nvd.nist.gov/vuln/detail/CVE-2020-13657

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

Identifikátor

Mozilla Firefox - viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje produkty Firefox a Firefox ESR, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.06.2020

CVE

CVE-2020-12402, CVE-2020-12415, CVE-2020-12416, CVE-2020-12417, CVE-2020-12418, CVE-2020-12419, CVE-2020-12420, CVE-2020-12421, CVE-2020-12422, CVE-2020-12423, CVE-2020-12424, CVE-2020-12425, CVE-2020-12426

Zasiahnuté systémy

Firefox verzie staršie ako 78
Firefox ESR verzie staršie ako 68.10

Následky

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

Odporúčania

Administrátorom 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 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.mozilla.org/en-US/security/advisories/mfsa2020-25/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-24/

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

Identifikátor

Microsoft Windows Codecs Library - zraniteľnosti

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje operačné systémy Windows 10 a Windows Server, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti v komponente Codecs Library umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.06.2020

CVE

CVE-2020-1425, CVE-2020-1457

Zasiahnuté systémy

Microsoft Windows

Následky

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

Odporúčania

Administrátorom 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 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://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1425
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1457
https://www.zdnet.com/article/microsoft-releases-emergency-security-update-to-fix-two-bugs-in-windows-codecs/
https://www.bleepingcomputer.com/news/security/microsoft-releases-oob-security-updates-for-windows-10-rce-bugs/
https://borncity.com/win/2020/07/01/windows-10-critical-codec-vulnerabilities-patched/

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

Identifikátor

Netgear produkty - viacero zraniteľností

Popis

Spoločnosť Netgear vydala bezpečnostné aktualizácie na portfólio svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.06.2020

CVE

-

Zasiahnuté systémy

D6220 firmware verzie staršie ako 1.0.0.56, D6400 firmware verzie staršie ako 1.0.0.90
D7000v2 firmware verzie staršie ako 1.0.0.58, D8500 firmware verzie staršie ako 1.0.3.46
DC112A firmware verzie staršie ako 1.0.0.46
EX3700, EX3800, EX3920 firmware verzie staršie ako 1.0.0.80EX6120 firmware verzie staršie ako 1.0.0.50
EX6130 firmware verzie staršie ako 1.0.0.32, EX6920 firmware verzie staršie ako 1.0.0.50
EX7000 firmware verzie staršie ako 1.0.1.86, R6250 firmware verzie staršie ako 1.0.4.40
R6400v2, R6700v3 firmware verzie staršie ako 1.0.4.94
R6900 firmware verzie staršie ako 1.0.2.12, R6900P firmware verzie staršie ako 1.3.2.120
R7000 firmware verzie staršie ako 1.0.11.102, R7000P firmware verzie staršie ako 1.3.2.120
R7100LG firmware verzie staršie ako 1.0.0.54, R7850 firmware verzie staršie ako 1.0.5.58
R7900 firmware verzie staršie ako 1.0.4.24, R8000 firmware verzie staršie ako 1.0.4.56
R8500 firmware verzie staršie ako 1.0.2.131, RS400 firmware verzie staršie ako 1.5.0.46
WNR3500Lv2 firmware verzie staršie ako 1.2.0.60, XR300 firmware verzie staršie ako 1.0.3.44

Doposiaľ neaktualizované:
AC1450, D6300, DGN2200, DGN2200M, DGND3700, EX6000, EX6100, EX6150, EX6200, LG2200D, MBM621, MBR1200, MBR1515, MBR1516, MBR624GU, MBRN3000, MVBR1210C, R4500, R6200, R6200v2, R6300, R6300v2, R6400, R6700, R7300, R8300, WGR614v10, WGR614v8, WGR614v9, WGT624v4, WN2500RP, WN2500RPv2, WN3000RP, WN3100RP, WN3500RP, WNCE3001, WNDR3300, WNDR3300v2, WNDR3400, WNDR3400v2, WNDR3400v3, WNDR3700v3, WNDR4000, WNDR4500, WNDR4500v2, WNR1000v3, WNR2000v2, WNR3500, WNR3500L, WNR3500v2, WNR834Bv2

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL). Tiež odporúčame zabezpečiť systémy podľa odporúčaní výrobcu a vypnúť funkciu vzdialenej správy.
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://kb.netgear.com/000061982/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Routers-Mobile-Routers-Modems-Gateways-and-Extenders
https://blog.grimm-co.com/2020/06/soho-device-exploitation.html
https://github.com/grimm-co/NotQuite0DayFriday/blob/master/2020.06.15-netgear/exploit.py
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-netgear-products-could-allow-for-remote-code-execution_2020-087/
https://www.zdnet.com/article/unpatched-vulnerability-identified-in-79-netgear-router-models/
https://www.zerodayinitiative.com/advisories/ZDI-20-703/
https://www.zerodayinitiative.com/advisories/ZDI-20-704/
https://www.zerodayinitiative.com/advisories/ZDI-20-705/
https://www.zerodayinitiative.com/advisories/ZDI-20-708/
https://www.zerodayinitiative.com/advisories/ZDI-20-709/
https://www.zerodayinitiative.com/advisories/ZDI-20-713/
https://www.zerodayinitiative.com/advisories/ZDI-20-711/
https://www.zerodayinitiative.com/advisories/ZDI-20-706/
https://www.zerodayinitiative.com/advisories/ZDI-20-712/
https://www.zerodayinitiative.com/advisories/ZDI-20-707/

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

Identifikátor

Cisco produkty viacero zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na portfólio svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v Small Business Smart and Managed Switches je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať kontrolu nad systémom.

Dátum prvého zverejnenia varovania

01.07.2020

CVE

CVE-2020-3282, CVE-2020-3297, CVE-2020-3340, CVE-2020-3391, CVE-2020-3402, CVE-2020-3420, CVE-2020-3431, CVE-2020-3432

Zasiahnuté systémy

Cisco 250 Series Smart Switches firmware verzie staršie ako 2.5.5.47
Cisco 350 Series Managed Switches firmware verzie staršie ako 2.5.5.47
Cisco 350X Series Stackable Managed Switches firmware verzie staršie ako 2.5.5.47
Cisco 550X Series Stackable Managed Switches firmware verzie staršie ako 2.5.5.47
Cisco Small Business 200 Series Smart Switches
Cisco Small Business 300 Series Managed Switches
Cisco Small Business 500 Series Stackable Managed Switches
Cisco Small Business RV042 and RV042G Routers firmware verzie staršie ako 4.2.3.14
Cisco AnyConnect Secure Mobility Client for Mac OS verzie staršie ako 4.9.00086
Cisco Unified Communications Manager (Unified CM) verzie staršie ako 10.5(2)SU10 a 11.5(1)SU8
Cisco Unified Communications Manager Session Management Edition (Unified CM SME) verzie staršie ako 10.5(2)SU10 a 11.5(1)SU8
Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) verzie staršie ako 10.5(2)SU10 a 11.5(1)SU8
Cisco Unified CVP verzie staršie ako 12.5(1)
Cisco Unity Connection verzie staršie ako 10.5(2)SU10 a 11.5(1)SU8
Cisco DNA Center verzie staršie ako 1.2.10
Cisco ISE verzie staršie ako 2.6 Patch 7

Následky

Neoprávnený prístup do systému, Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbswitch-session-JZAS5jnY
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-mac-dos-36s2y3Lv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-cuc-imp-xss-OWuSYAp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-bLZw4Ctq
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cvp-info-dislosure-NZBEwj9V
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-info-disc-6xsCyDYy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mlt-ise-strd-xss-nqFhTtx7
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sa-rv-routers-xss-K7Z5U6q3
https://threatpost.com/cisco-warns-high-severity-bug-small-business-switch/157090/

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

Identifikátor

PHOENIX CONTACT PC Worx - zraniteľnosti

Popis

Bezpečnostní výskumníci informovali o zraniteľnostiach v produkte Phoenix Contact PC Worx a PC Worx Express.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených .xml a .mwe súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.07.2020

CVE

CVE-2020-12497, CVE-2020-12498

Zasiahnuté systémy

Phoenix Contact PC Worx verzie 1.87 a staršie
Phoenix Contact PC Worx Express verzie 1.87 a staršie

Následky

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

Odporúčania

Spoločnosť Phoenix Contact doposiaľ nevydala bezpečnostné aktualizácie riešiace uvedené zraniteľnosti. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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.

Zdroje

https://cert.vde.com/en-us/advisories/vde-2020-023

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

Identifikátor

Delta Electronics DOPSoft - zraniteľnosti

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt DOPSoft, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.06.2020

CVE

CVE-2020-10597, CVE-2020-14482

Zasiahnuté systémy

Delta Electronics Delta Industrial Automation DOPSoft verzie staršie ako 4.00.08.17

Následky

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

Odporúčania

Administrátorom 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.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-20-182-01
https://nvd.nist.gov/vuln/detail/CVE-2020-14482

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

Identifikátor

Check Point ZoneAlarm - zraniteľnosť

Popis

Spoločnosť Check Point vydala bezpečnostnú aktualizáciu na svoj produkt ZoneAlarm, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

24.06.2020

CVE

CVE-2020-6013

Zasiahnuté systémy

Check Point ZoneAlarm verzie staršie ako 15.8.109.18436

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-20-803/
https://www.zonealarm.com/software/extreme-security/release-history

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

Identifikátor

Mitsubishi Electric Factory Automation - viacero zraniteľností

Popis

Spoločnosť Mitsubishi Electric vydala aktualizácie pre svoje produkty Factory Automation, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne upravených XML súborov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

30.06.2020

CVE

CVE-2020-5602, CVE-2020-5603

Zasiahnuté systémy

CPU Module Logging Configuration Tool verzie staršie ako 1.100E
CW Configurator verzie staršie ako 1.011M
EM Software Development Kit (EM Configurator) verzie staršie ako 1.015R
GT Designer3GOT2000) verzie staršie ako 1.225K
GX LogViewer verzie staršie ako 1.100E
GX Works2 verzie staršie ako 1.590Q
GX Works3 verzie staršie ako 1.060N
M_CommDTM-HART verzie staršie ako 1.01B
M_CommDTM-IO-Link verzie staršie ako 1.03D
MELFA-Works verzie staršie ako 4.4
MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool verzie staršie ako 1.005F
MELSOFT FieldDeviceConfigurator verzie staršie ako 1.04E
MELSOFT iQ AppPortal verzie staršie ako 1.14Q
MELSOFT Navigator verzie staršie ako 2.62Q
MI Configurator verzie staršie ako 1.004E
Motion Control Setting verzie staršie ako 1.006G
MR Configurator2 verzie staršie ako 1.100E
MT Works2 verzie staršie ako 1.160S
RT ToolBox2 verzie staršie ako 3.73B
RT ToolBox3 verzie staršie ako 1.60N

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje
https://www.us-cert.gov/ics/advisories/icsa-20-182-02 https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-004_en.pdf https://jvn.jp/en/vu/JVNVU90307594/index.html

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-171