BEZPEČNOSTNÝ BULLETIN

Týždeň 17. 02. 2021 - 23. 02. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Bezpečnostné zraniteľnosti v produkte Nagios XI	Vysoká	**8.8**
02.	Viacero bezpečnostných zraniteľností v produkte Advantech WebAccess	Vysoká	**8.8**
03.	Bezpečnostná zraniteľnosť v produkte Apache MyFaces	Vysoká	**8.8**
04.	Viacero bezpečnostných zraniteľností v produkte Google Chrome	Vysoká	**8.0**
05.	Bezpečnostná zraniteľnosť knižnice avahi-daemon	Vysoká	**7.8**
06.	Viacero bezpečnostných zraniteľností v produktoch Open Design Alliance	Vysoká	**7.8**
07.	Bezpečnostná zraniteľnosť v produkte Cisco AnyConnect	Vysoká	**7.8**
08.	Bezpečnostná zraniteľnosť v produkte Rockwell Automation Allen-Bradley Micrologix	Vysoká	**7.5**
09.	Dve bezpečnostné zraniteľnosti v produktoch Mitsubishi Electric	Vysoká	**7.5**
10.	Bezpečnostná zraniteľnosť v produktoch Johnson Controls	Vysoká	**7.5**
11.	Bezpečnostná zraniteľnosť v module Node.js lodash	Vysoká	**7.2**

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-343

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

Identifikátor

Bezpečnostné zraniteľnosti v produkte Nagios XI

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Nagios XI.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.02.2021

CVE

CVE-2021-25296, CVE-2021-25297, CVE-2021-25298

Zasiahnuté systémy

Nagios Nagios XI vo verzii staršej ako 5.7.5 (vrátane)

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dotupné aktualizácie. Administrátorom 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://exchange.xforce.ibmcloud.com/vulnerabilities/196790
https://exchange.xforce.ibmcloud.com/vulnerabilities/196791
https://exchange.xforce.ibmcloud.com/vulnerabilities/196792
https://github.com/fs0c-sh/nagios-xi-5.7.5-bugs/blob/main/README.md
https://assets.nagios.com/downloads/nagiosxi/versions.php

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

Identifikátor

Viacero bezpečnostných zraniteľností v produkte Advantech WebAccess

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na produkt WebAccess/SCADA, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na zasiahnutom systéme a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.02.2021

CVE

CVE-2020-13550, CVE-2020-13551, CVE-2020-13552, CVE-2020-13553, CVE-2020-13554, CVE-2020-13555

Zasiahnuté systémy

Advantech WebAccess/SCADA vo verzii staršej ako 9.0.2

Následky

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

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://talosintelligence.com/vulnerability_reports/TALOS-2020-1169
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1168
https://www.advantech.com/support/details/manual?id=1-1J6QG9J

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Apache MyFaces

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt MyFaces, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webstránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.02.2021

CVE

CVE-2021-26296

Zasiahnuté systémy

Apache MyFaces vo verzii staršej ako 3.0.0-RC1 (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.
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://seclists.org/oss-sec/2021/q1/159
https://exchange.xforce.ibmcloud.com/vulnerabilities/197017
https://github.com/apache/myfaces/pull/134

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Viacero bezpečnostných zraniteľností v produkte Google Chrome

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.02.2021

CVE

CVE-2021-21149, CVE-2021-21150, CVE-2021-21151, CVE-2021-21152, CVE-2021-21153, CVE-2021-21154, CVE-2021-21155, CVE-2021-21156, CVE-2021-21157

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 88.0.4324.182

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.
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://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2021-026/
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
https://www.auscert.org.au/bulletins/ESB-2021.0581

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

Identifikátor

Bezpečnostná zraniteľnosť knižnice avahi-daemon

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti knižnice avahi-daemon pre Debian. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom špeciálne vytvoreného odkazu eskalovať svoje privilégiá na zasiahnutom systéme a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.02.2021

CVE

CVE-2021-26720

Zasiahnuté systémy

Debian avahi-daemon vo verzii staršej ako 0.7-4

Následky

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

Odporúčania

Administrátorom 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/196796
https://seclists.org/oss-sec/2021/q1/142
https://packages.debian.org/buster/avahi-daemon
https://bugzilla.suse.com/show_bug.cgi?id=1180827

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

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch Open Design Alliance

Popis

Spoločnosť Open Design Alliance vydala bezpečnostnú aktualizáciu na svoj produkt Drawings SDK, 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

16.02.2021

CVE

CVE-2021-25173, CVE-2021-25174, CVE-2021-25175, CVE-2021-25176, CVE-2021-25177, CVE-2021-25178

Zasiahnuté systémy

Drawings SDK vo verzii staršej ako 2021.12

Následky

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

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 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://us-cert.cisa.gov/ics/advisories/icsa-21-047-01
https://www.opendesign.com/products/drawings

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Cisco AnyConnect

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt AnyConnect Secure Mobility Client, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom narušenia komunikácie medzi procesmi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.02.2021

CVE

CVE-2021-1366

Zasiahnuté systémy

Cisco AnyConnect Secure Mobility Client pre Windows vo verzii staršej ako 4.9.05042 s nainštalovaným modulom VPN Posture

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.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-hijac-JrcTOQMC
https://exchange.xforce.ibmcloud.com/vulnerabilities/196966

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Rockwell Automation Allen-Bradley Micrologix

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt Allen-Bradley Micrologix, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.02.2021

CVE

CVE-2020-6111

Zasiahnuté systémy

Allen-Bradley MicroLogix vo verzii staršej ako 1400 s nainštalovaným firmware vo verzii staršej ako v21.006

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-047-02

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

Identifikátor

Dve bezpečnostné zraniteľnosti v produktoch Mitsubishi Electric

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.02.2021

CVE

CVE-2021-20587, CVE-2021-20588

Zasiahnuté systémy

C Controller module setting and monitoring tool všetky verzie
CPU Module Logging Configuration Tool všetky verzie
CW Configurator všetky verzie
Data Transfer všetky verzie
EZSocket všetky verzie
FR Configurator všetky verzie
FR Configurator SW3 všetky verzie
FR Configurator2 všetky verzie
GT Designer3 Version1(GOT1000) všetky verzie
GT Designer3 Version1(GOT2000) všetky verzie
GT SoftGOT1000 všetky verzie
GT SoftGOT2000 všetky verzie
GX Configurator-DP vo verzii staršej ako 7.15R
GX Configurator-QP všetky verzie
GX Developer všetky verzie
GX Explorer všetky verzie
GX IEC Developer všetky verzie
GX LogViewer všetky verzie
GX RemoteService-I všetky verzie
GX Works2 vo verzii staršej ako 1.600A
GX Works3 vo verzii staršej ako 1.072A
M_CommDTM-HART všetky verzie
M_CommDTM-IO-Link všetky verzie
MELFA-Works všetky verzie
MELSEC WinCPU Setting Utility všetky verzie
MELSOFT EM Software Development Kit (EM Configurator) všetky verzie
MELSOFT Navigator všetky verzie
MH11 SettingTool šetky verzie
MI Configurator všetky verzie
MT Works2 všetky verzie
MX Component všetky verzie
Network Interface Board CC IE Control utility všetky verzie
Network Interface Board CC IE Field Utility všetky verzie
Network Interface Board CC-Link Ver.2 Utility všetky verzie
Network Interface Board MNETH utility všetky verzie
PX Developer všetky verzie
RT ToolBox2 všetky verzie
RT ToolBox3 všetky verzie
Setting/monitoring tools for the C Controller module všetky verzie
SLMP Data Collector všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Taktiež odporúčame produkty prevádzkovať pod účtom, ktorý nemá administrátorské oprávnenia.
V prípade, že je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-049-02

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Johnson Controls

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na svoj produkt Metasys Reporting Engine Web Services, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

18.02.2021

CVE

CVE-2020-9050

Zasiahnuté systémy

Metasys Reporting Engine Web Services vo verzii staršej ako v2.2

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom 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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-049-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v module Node.js lodash

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti modulu Node.js lodash.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s administrátorskými právomocami prostredníctvom zasielania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.02.2021

CVE

CVE-2021-23337

Zasiahnuté systémy

Node.js lodash vo verzii staršej ako 4.17.20 (vrátane)

Následky

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

Odporúčania

Odporúčame usitiť sa, či Vaše aplikácie nevyužívajú modul lodash v zraniteľnej verzii. V prípade, že áno, 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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/196797
https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932
https://www.npmjs.com/package/lodash

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-343