BEZPEČNOSTNÉ VAROVANIE

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.8**
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.
Najzávažnejšie bezpečnostné zraniteľnosti v Cisco IOS a IOS XE umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.06.2020

CVE

CVE-2020-3198, CVE-2020-3199, CVE-2020-3200, CVE-2020-3201, CVE-2020-3203, CVE-2020-3204,
CVE-2020-3206, CVE-2020-3207, CVE-2020-3208, CVE-2020-3209, CVE-2020-3210, CVE-2020-3211,
CVE-2020-3212, CVE-2020-3213, CVE-2020-3214, CVE-2020-3215, CVE-2020-3216, CVE-2020-3217,
CVE-2020-3218, CVE-2020-3219, CVE-2020-3220, CVE-2020-3221, CVE-2020-3222, CVE-2020-3223,
CVE-2020-3224, CVE-2020-3225, CVE-2020-3226, CVE-2020-3227, CVE-2020-3228, CVE-2020-3229,
CVE-2020-3230, CVE-2020-3231, CVE-2020-3232, CVE-2020-3233, CVE-2020-3234, CVE-2020-3235,
CVE-2020-3237, CVE-2020-3238, CVE-2020-3257, CVE-2020-3258, CVE-2020-3267, CVE-2020-3281,
CVE-2020-3333, CVE-2020-3335, CVE-2020-3339, CVE-2020-3353

IOC

-

Zasiahnuté systémy

Cisco IOS XE Software verzie 16.3.1 a staršie
Cisco IOS
Cisco NX-OS
Cisco 809 and 829 Industrial ISRs
Cisco Catalyst 3650 Series Switches
Cisco Catalyst 3850 Series Switches
Cisco Catalyst 9200 Series Switches
Cisco Catalyst 9300 Series Switches
Cisco Catalyst 9500 Series Switches
Cisco Catalyst 9800 Series Wireless Controllers
Cisco Catalyst 9800-L Wireless Controllers
Cisco Nexus 3000 Series Switches
Cisco Nexus 5500 Platform Switches
Cisco Nexus 5600 Platform Switches
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9000 Series Switches in standalone NX-OS mode
Cisco IOx Application Framework verzie staršie ako 1.9.0

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-136

Cisco 800 Series Industrial Integrated Services Routers (Industrial ISRs)
Cisco 800 Series Integrated Services Routers (ISRs)
Cisco 1000 Series Connected Grid Routers (CGR1000) Compute Module
Cisco IC3000 Industrial Compute Gateway
Cisco Industrial Ethernet (IE) 4000 Series Switches
Cisco 1000 Series ISRs
Cisco 4000 Series ISRs
Cisco 4300 Series ISRs
Cisco ASR 1000 Series Aggregation Services Routers
Cisco Catalyst 9x00 Series Switches
Cisco Catalyst IE3400 Rugged Series Switches
Cisco Embedded Services 3300 Series Switches
Cisco IR510 WPAN Industrial Routers
Cisco Unified CCX software verzie staršie ako 12.5(1)
Cisco Prime Infrastructure verzie staršie ako 3.7.1 Update 01 a 3.8 Update 02
Cisco ISE verzie staršie ako 2.2.0.470-Patch13,2.3.0.298-Patch6 a 2.4.0.357-Patch2
Cisco Application Services Engine Software verzie staršie ako 1.1.2.20.
Cisco ASR 920 Series Aggregation Services Router model ASR920-12SZ-IM
Cisco DNA Center software verzie staršie ako 1.3.3.3.

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. V prípade, ak na zraniteľných zariadeniach nepoužívate IOx prostredie a HTTP server, odporúčame ich v nastaveniach zariadenia vypnúť príkazmi "no iox", "no ip http server" a "no ip http secure-server".
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-ioxPE-KgGvCAf9
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-rce-xYRSeMNH
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-cmdinj-zM283Zdw
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-PZgQxjfG
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-web-cmdinj4-S2TmH7GA
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-web-cmdinj3-44st5CcA
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssh-dos-Un22sd2A
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ikev2-9p23Jj2a
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sxp-68TEVzR
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-vpn-dos-edOmW28Z
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr920-ABjcLmef
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-dos-AnvKvMxR
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-APIC-KSV-3wzbHYT4
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-caf-file-mVnPqKW9
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-audit-log-59RBdwb6
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c2960L-DpWA9Re4
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-auth-b-NzwhJHH7

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-priv-esc3-GMgnGCHx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxxss-wc6CqUws
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-APIC-EPU-F8y5kUOP
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-dos-qNzq39K7
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-priv-esc2-A6jVRu7C
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-sql-inj-KGLLsFw8
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-priv-esc1-OKMKFRhV
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-api-auth-WSx4v7sB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tcl-ace-C9KuVKmm
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-web-cmdinj2-fOnjk2LD
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tcl-dos-MAZQUnMF
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-dos-USxSyTk5
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-filerd-HngnDYGk
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-gos-vuln-s9qS8kYL
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sip-Cv28sQw2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ngwc-cmdinj-KEwWVWR
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ewlc-dos-TkuPVmZN
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-caf-3dXM8exv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cipdos-hkfTZXEx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-rce-uk8BXcUD
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-unauthprxy-KXXsbWh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-nxos-onepk-rce-6Hhyt4dC
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-vds-cmd-inj-VfJtqGhE
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-fnfv9-dos-HND6Fc9u
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-ir800-img-verif-wHhLYHjK
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-digsig-bypass-FYQ3bmVq
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-vds-cred-uPMp9zbY