BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 10. 2020 - 03. 11. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

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-266

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

Identifikátor

Zraniteľnosti v Adobe Acrobat DC a Adobe DC

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Acrobat DC a Adobe DC, ktoré opravujú viaceré bezpečnostné zraniteľnosti.
Najzávažnejšia zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného PDF súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.11.2020

CVE

CVE-2020-24426, CVE-2020-24427, CVE-2020-24428, CVE-2020-24429, CVE-2020-24430, CVE-2020-24431, CVE-2020-24432, CVE-2020-24433, CVE-2020-24434, CVE-2020-24435, CVE-2020-24436, CVE-2020-24437, CVE-2020-24438, CVE-2020-24439

Zasiahnuté systémy

Acrobat DC verzie 2020.012.20048 a staršie
Acrobat Reader DC verzie 2020.012.20048 a staršie
Acrobat 2020 verzie 2020.001.30005 and earlier versions
Acrobat Reader 2020 verzie 2020.001.30005 and earlier versions
Acrobat 2017 verzie 2017.011.30175 a staršie
Acrobat Reader 2017 verzie 2017.011.30175 a staršie

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 zraniteľnosti, 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://helpx.adobe.com/security/products/acrobat/apsb20-67.html
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1157

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

Identifikátor

Viacero zraniteľností v Cisco produktoch

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkty AnyConnect Mobility Client, IOS XR Software Enchanced PXE boot loader, Webex Network Recording Player, Webex Player a SD-WAN Software, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť sa nachádza v produkte PXE boot loader a umožňuje vzdialenému neautentifikovanému útočníkovi počas PXE boot procesu vykonanie škodlivého kódu vedúceho k úplnému narušeniu dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.11.2020

CVE

CVE-2020-26071, CVE-2020-26073, CVE-2020-26074, CVE-2020-3284, CVE-2020-3556, CVE-2020-3573, CVE-2020-3574, CVE-2020-3593, CVE-2020-3594, CVE-2020-3595, CVE-2020-3600, CVE-2020-3603, CVE-2020-3604

Zasiahnuté systémy

AnyConnect Secure Mobility Client pre Linux
AnyConnect Secure Mobility Client pre MacOS
AnyConnect Secure Mobility Client pre Windows
Cisco ASR 9000 Series A9K-RSP880-SE verzie staršie ako 6.5.2 s Biosom starším ako 10.65
Cisco ASR 9000 Series A9K-RSP880-TR verzie staršie ako 6.5.2 s Biosom starším ako 10.65
ACisco ASR 9000 Series 99-RP2-SE verzie staršie ako 6.5.2 s Biosom starším ako 14.35
Cisco ASR 9000 Series A99-RP2-TR verzie staršie ako 6.5.2 s Biosom starším ako 14.35
Cisco ASR 9000 Series A99-RSP-SE verzie staršie ako 6.5.2 s Biosom starším ako 16.14
Cisco ASR 9000 Series A99-RSP-TR verzie staršie ako 6.5.2 s Biosom starším ako 16.14
Cisco ASR 9000 Series A9K-RSP880-LT-SE verzie staršie ako 6.5.2 s Biosom starším ako 17.34
Cisco ASR 9000 Series A9K-RSP880-LT-TR verzie staršie ako 6.5.2 s Biosom starším ako 17.34
Cisco ASR 9000 Series ASR-9901-RP verzie staršie ako 6.5.2 s Biosom starším ako 22.20
Cisco ASR 9000 Series A99-RP3-SE verzie staršie ako 6.5.2 s Biosom starším ako 30.23
Cisco ASR 9000 Series A99-RP3-TR verzie staršie ako 6.5.2 s Biosom starším ako 30.23
Cisco ASR 9000 Series A9K-RSP5-SE verzie staršie ako 6.5.2 s Biosom starším ako 31.20
Cisco ASR 9000 Series A9K-RSP5-TR verzie staršie ako 6.5.2 s Biosom starším ako 31.20
Cisco NCS 1000 NCS1001 verzie staršie ako 7.1.1 s Biosom starším ako 14.60
Cisco NCS 1000 NCS1002 verzie staršie ako 7.1.1 s Biosom starším ako 14.60
Cisco NCS 1000 NCS1004 verzie staršie ako 7.1.1 s Biosom starším ako 14.60
Cisco NCS 540 N540-12Z20G-SYS-A/D verzie staršie ako 7.2.1 s Biosom starším ako 1.15
Cisco NCS 540 N540-24Z8Q2C-M verzie staršie ako 7.2.1 s Biosom starším ako 1.15
Cisco NCS 540 N540-28Z4C-SYS-A/D verzie staršie ako 7.2.1 s Biosom starším ako 1.15
Cisco NCS 540 N540-ACC-SYS verzie staršie ako 7.2.1 s Biosom starším ako 1.15
Cisco NCS 540 N540X-16Z4G8Q2C-A/D verzie staršie ako 7.2.1 s Biosom starším ako 1.15
Cisco NCS 540 N540X-12Z16G-SYS-A/D verzie staršie ako 7.2.1 s Biosom starším ako 1.15
Cisco NCS 560 N560-4-SYS verzie staršie ako 6.6.3, 6.6.25, a 7.0.2 s Biosom starším ako 0.14
Cisco NCS 560 N560-7-SYS verzie staršie ako 6.6.3, 6.6.25, a 7.0.2 s Biosom starším ako 0.14
Cisco NCS 5000 NCS5001 verzie staršie ako 7.2.1 s Biosom starším ako 1.13
Cisco NCS 5000 NCS5002 verzie staršie ako 7.2.1 s Biosom starším ako 1.13
Cisco NCS 5000 NCS5011 verzie staršie ako 7.2.1 s Biosom starším ako 1.14
NC55-RP verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 9.30
NC55-RP-E verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.21
NCS-5501 verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.21
NCS-5501-SE verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.21
NCS-5502 verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.21
NCS-5502-SE verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.21
NCS-55A2-MOD-S verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.12
NCS-55A2-MOD-HD-S verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.12
NCS-55A2-MOD-HX-S verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.12
NCS-55A2-MOD-SE-S verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.12
NCS-55A2-MOD-SE-H-S verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.12
NCS-55A1-36H-SE-S verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.12
NCS-55A1-36H-S verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.12
NCS-55A1-24H verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.12
NCS55-A1-48Q6H verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.12
NCS-55A1-24Q6H-S verzie staršie ako 6.6.3 a 6.6.25 s Biosom starším ako 1.12
Webex Meetings 40.6.x sites verzie staršie ako 40.6.11
Webex Meetings sites verzie staršie ako 40.8.0
Webex Meetings Server 3.x verzie staršie ako 3.0MR3 SP4
Webex Meetings Server 4.x verzie staršie ako 4.0MR3 SP3
Cisco SD-WAN verzie staršie ako a 20.1.2
IP DECT 210 Multi-Cell Base Station with Multiplatform Firmware verzie staršie ako 4.8.1
IP DECT 6825 with Multiplatform Firmware verzie staršie ako 4.8.1
IP Phone 8811 Series with Multiplatform Firmware verzie staršie ako 11.3.2
IP Phone 8841 Series with Multiplatform Firmware verzie staršie ako 11.3.2
IP Phone 8851 Series with Multiplatform Firmware verzie staršie ako 11.3.2
IP Phone 8861 Series with Multiplatform Firmware verzie staršie ako 11.3.2
Unified IP Conference Phone 8831 for Third-Party Call Control zatiaľ neaktualizované
Webex Room Phone verzie staršie ako 1.2.0

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

Odporúčania
Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Po odstránení zraniteľnosti, 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-vsoln-arbfile-gtsEYxns https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-ipc-KfQO9QhK https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pxe-unsign-code-exec-qAa78fD2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-nbr-NOS6FQ24 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vsoln-arbfile-gtsEYxns https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-flood-dos-YnU9EXOv https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-escalation-Jhqs5Skf https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-traversal-hQh24tmk https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepestd-8C3J9Vc https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepeshlg-tJghOQcA https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepescm-BjgQm4vJ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepegr-4xynYLUj https://tools.cisco.com/security/center/publicationListing.x

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

Identifikátor

Bezpečnostná aktualizácia na herný klient EA Origin

Popis

Spoločnosť EA vydala bezpečnostnú aktualizáciu na svojho herného klienta Origin pre Mac & PC, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť umožňuje lokálnemu autentifikovanému útočníkovi s používateľskými právami prostredníctvom použitia špeciálne vytvoreného Qt pluginu eskalovať svoje privilégiá na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

28.10.2020

CVE

CVE-2020-27708

Zasiahnuté systémy

Origin pre Mac & PC verzie staršie ako 10.5.86

Následky

Eskalácia privilégií

Odporúčania

Používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.ea.com/security/news/easec-2020-002-elevation-of-privilege-vulnerability-in-origin-client

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť softwaru Cisco Webex Meetings

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj videokonferenčný software Webex Meetings, ktorá opravuje bezpečnostnú zraniteľnosť zneužiteľnú pri spúšťaní aplikácie vo virtuálnom prostredí.
Zraniteľnosť umožňuje lokálnemu autentifikovanému útočníkovi prostredníctom zasielania špeciálne vytvorených správ zmeniť nastavenie operačného systému a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.11.2020

CVE

CVE-2020-3588

Zasiahnuté systémy

Cisco Webex Meetings pre Windows vo verziách starších ako 40.6.9 a 40.8.9

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 zraniteľnosti, 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-vdi-qQrpBwuJ

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v Linuxovom jadre (kernel)

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti komponentu "KVM Hypervisor" v linuxovom jadre.
Zraniteľnosť umožňuje lokálnemu autentifikovanému útočníkovi spôsobiť rekurzívne vyčerpanie zásobníka a následné zneprístupnenie služby.

Dátum prvého zverejnenia varovania

03.11.2020

CVE

CVE-2020-27152

Zasiahnuté systémy

CVE-2020-27152

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.openwall.com/lists/oss-security/2020/11/03/1
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=77377064c3a94911339f13ce113b3abf265e06da