BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 02. 2018 – 06. 03. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Delta Electronics Products Multiple Vulnerabilities

Popis

Spoločnosť Delta Electronics vydala bezpečnostné aktualizácie na svoje produkty WPLSoft a DOPSoft, ktoré opravujú viacero spoločnosťou bližšie nešpecifikovaných bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému útočníkovi spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

27.02.2018

CVE

CVE-2018-5476, CVE-2018-7494, CVE-2018-7507, CVE-2018-7509

Zasiahnuté systémy

WPLSoft verzia 2.45.0 a staršie
Delta Industrial Automation DOPSoft verzia 4.00.01 a staršie

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-058-02
https://ics-cert.us-cert.gov/advisories/ICSA-18-060-03

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

Identifikátor

Philips Intellispace Portal ISP Vulnerabilities

Popis

Spoločnosť Philips vydala oznámenie o viacerých bezpečnostných zraniteľnostiach vo svojom produkte Philips' IntelliSpace Portal (ISP).
Najvážnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a nedostatočnej autentifikácii používateľských vstupov a umožňujú vzdialenému útočníkovi vykonať škodlivý kód, získať prístup k citlivým údajom a spôsobiť odopretie služieb.

Dátum prvého zverejnenia varovania

26.02.2018

CVE

CVE-2004-2761, CVE-2005-1794, CVE-2011-3389, CVE-2014-3566, CVE-2016-2183, CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148, CVE-2017-0199, CVE-2017-0267, CVE-2017-0268, CVE-2017-0269, CVE-2017-0270, CVE-2017-0271, CVE-2017-0272, CVE-2017-0273, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279, CVE-2017-0280, CVE-2018-5454, CVE-2018-5458, CVE-2018-5462, CVE-2018-5464, CVE-2018-5466, CVE-2018-5468, CVE-2018-5470, CVE-2018-5472, CVE-2018-5474

Zasiahnuté systémy

IntelliSpace Portal, verzie 8.0.x
IntelliSpace Portal, verzie 7.0.x

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti

Odporúčania

Spoločnosť Philips doposiaľ nevydala bezpečnostné aktualizácie uvedených produktov. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu softvéru. Spoločnosť Philips umožňuje používateľom zasiahnutých produktov využiť svoje InCenter konto na adrese http://incenter.medical.philips.com na získanie dodatočných odporúčaní, ako zabrániť zneužitiu daných zraniteľností.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02

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

Identifikátor

Emerson ControlWave Micro Process Automation Controller Vulnerability

Popis

Spoločnosť Emerson vydala bezpečnostnú aktualizáciu na svoj produkt ControlWave Micro Process Automation Controller, ktorá opravuje spoločnosťou bližšie nešpecifikovanú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi prostredníctvom požiadaviek na porte 20547 spôsobiť pretečenie zásobníka a zneprístupnenie ethernetových služieb napadnutých zariadení.

Dátum prvého zverejnenia varovania

27.02.2018

CVE

CVE-2018-5452

Zasiahnuté systémy

ControlWave Micro [ProConOS v.4.01.280] firmware: CWM v.05.78.00 a staršie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-058-03
https://www.securityweek.com/emerson-patches-severe-flaw-controlwave-controllers

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

Identifikátor

dhclient Buffer Overflow Vulnerability

Popis

Vývojári DHCP klienta dhclient vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi vydávajúcemu sa za server prostredníctvom podvrhnutia špeciálne upravených DHCP odpovedí spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód, prípadne spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.02.2018

CVE

CVE-2018-5732, CVE-2018-5733

Zasiahnuté systémy

DHCP verzie 4.1.0 až 4.1-ESV-R15, 4.2.0 až 4.2.8, 4.3.0 až 4.3.6, 4.4.0

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://kb.isc.org/article/AA-01565/75/CVE-2018-5732
https://kb.isc.org/article/AA-01567/75/CVE-2018-5733
https://www.securitytracker.com/id/1040436
https://tools.cisco.com/security/center/viewAlert.x?alertId=56972
https://tools.cisco.com/security/center/viewAlert.x?alertId=56973

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

Identifikátor

Big IP Multiple Vulnerabilities

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoje produkty Big IP, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšie bezpečnostné zraniteľnosti spočívajú v nesprávnom spracovaní dát v zasiahnutom systéme a umožňujú vzdialenému neautentifikovanému útočníkovi zasielaním špeciálne upravených paketov spôsobiť odopretie služieb.

Dátum prvého zverejnenia varovania

02.03.2018

CVE

CVE-2017-6150, CVE-2017-6154, CVE-2018-5500, CVE-2018-5501

Zasiahnuté systémy

Big IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, GTM, Link Controller, PEM, WebAccelerator, WebSafe) vývojové vetvy 13.x, 12.x a 11.x verzie nižšie ako 13.1.0, 12.1.3.2, 11.6.3

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov

Zdroje

https://support.f5.com/csp/article/K62712037
https://support.f5.com/csp/article/K33211839
https://support.f5.com/csp/article/K44200194
https://support.f5.com/csp/article/K38243073

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

Identifikátor

BIND Assertion Failure in badcache.c

Popis

Vývojári DNS servera BIND vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v SERVFAIL cache komponente.
Bezpečnostná zraniteľnosť spočíva v chybnom uprednostnení funkcie SERVFAIL rcode namiesto funkcie FORMERR rcode pri spracovaní paketov a umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.02.2018

CVE

CVE-2018-5734

Zasiahnuté systémy

BIND verzie 9.10.5-S1 až 9.10.5-S4, 9.10.6-S1, 9.10.6-S2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov. Taktiež odporúčame zakázať komponent SERVFAIL cache prostredníctvom príkazu "servfail-ttl 0;" čím sa zablokuje možné zneužitie danej zraniteľnosti.

Zdroje

https://kb.isc.org/article/AA-01562/74/CVE-2018-5734
https://tools.cisco.com/security/center/viewAlert.x?alertId=56971

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Multiple SAML Libraries Authentication Bypass Vulnerability

Popis

Vývojári spoločnosti Duo Security informovali o novej triede zraniteľností, ktorými sú zasiahnuté autentifikačné systémy založené na jazyku SAML.
Bezpečnostné zraniteľnosti sú spôsobené nesprávnym používaním XML DOM API komponentov niektorými SAML knižnicami, v dôsledku čoho je vykonaná nesprávna syntaktická analýza a nekorektné zašifrovanie SAML správ.
Bezpečnostné zraniteľnosti umožňujú vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného SAML obsahu obísť primárne bezpečnostné mechanizmy poskytovateľov SAML služieb.

Dátum prvého zverejnenia varovania

06.02.2018 (posledná aktualizácia 27.02.2018)

CVE

CVE-2017-11427, CVE-2017-11428, CVE-2017-11429, CVE-2017-11430, CVE-2018-0489, CVE-2018-7340

Zasiahnuté systémy

OneLogin - python-saml
OneLogin - ruby-saml
Clever - saml2-js
OmniAuth-SAML
Shibboleth
Duo Network Gateway

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov a vývojárom SAML knižníc odporúčame preveriť možný výskyt uvedených zraniteľností v ich implementáciách.

Zdroje

https://duo.com/blog/duo-finds-saml-vulnerabilities-affecting-multiple-implementations
https://www.kb.cert.org/vuls/id/475445

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Network Time Protocol Multiple Vulnerabilities

Popis

Vývojári ntp.org vydali bezpečnostnú aktualizáciu svojho produktu Network Time Protocol, ktorá opravuje viacero bezpečnostných zraniteľností a chýb.
Najvážnejšie bezpečnostné zraniteľnosti spočívajúce v nedostatočnej implementácii bezpečnostných mechanizmov a nedostatočnej autentifikácii používateľských vstupov umožňujú vzdialenému útočníkovi vykonať škodlivý kód, získať prístup k citlivým údajom a spôsobiť odopretie služieb.

Dátum prvého zverejnenia varovania

27.02.2018

CVE

CVE-2018-7170, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185, CVE-2016-1549

Zasiahnuté systémy

Network Time Protocol 4.2 (.8p6, .8p7, .8p8, .8p9, .8p10)

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.vuxml.org/freebsd/af485ef4-1c58-11e8-8477-d05099c0ae8c.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=56952
https://tools.cisco.com/security/center/viewAlert.x?alertId=56955
https://tools.cisco.com/security/center/viewAlert.x?alertId=56953
https://tools.cisco.com/security/center/viewAlert.x?alertId=56950

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Memcached Network Message Volume Denial of Service Vulnerability

Popis

Vývojári softvéru Memcached vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje viacero chýb a bezpečnostnú zraniteľnosť v predvolených nastaveniach.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou kontrolou objemu dátového toku a umožňuje vzdialenému útočníkovi pomocou podvrhnutia upravených UDP požiadaviek vyvolať nevhodnú odozvu Memcached servera a zneužiť ho na vykonanie masívnych DDoS útokov voči iným cieľom.

Dátum prvého zverejnenia varovania

27.02.2018

CVE

CVE-2018-1000115

Zasiahnuté systémy

Memcached verzie nižšie ako 1.5.6

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a aplikáciu firewallových riešení, ktoré prístup k serveru umožnia iba z lokálnej siete a blokujú externú sieťovú prevádzku smerovanú na UDP port 11211.
Ak na serveri nie je nutné použitie UDP protokolu, odporúčame ho v nastaveniach servera deaktivovať a využívať spojovo orientovaný protokol TCP.

Zdroje

https://github.com/memcached/memcached/wiki/ReleaseNotes156
https://tools.cisco.com/security/center/viewAlert.x?alertId=57020