BEZPEČNOSTNÝ BULLETIN

Týždeň 31. 03. 2021 - 06. 04. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Apache Druid - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	VMware vRealize Operations Manager - dve bezpečnostné zraniteľnosti	Vysoká	**8.6**
04.	ZTE ZXHN F623 produkt - bezpečnostná zraniteľnosť	Vysoká	**8.6**
05.	BuddyPress plugin pre WordPress - bezpečnostná zraniteľnosť	Vysoká	**8.1**
06.	SolarWinds Orion Virtual Infrastructure Monitor - bezpečnostná zraniteľnosť	Vysoká	**7.8**
07.	ForgeRock OpenAM produkt - bezpečnostná zraniteľnosť	Vysoká	**7.5**
08.	MicroSeven MYM71080i-B produkt - bezpečnostná zraniteľnosť	Vysoká	**7.5**
09.	Bosch Rexroth ActiveMover - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
10.	cURL libcurl - bezpečnostná zraniteľnosť	Vysoká	**7.5**
11.	TP-Link produkty - bezpečnostná zraniteľnosť	Vysoká	**7.2**
12.	Microcosm bluemonday - bezpečnostná zraniteľnosť	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-381

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

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

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

Dátum prvého zverejnenia varovania

30.03.2021

CVE

CVE-2021-21194, CVE-2021-21195, CVE-2021-21196, CVE-2021-21197, CVE-2021-21198, CVE-2021-21199

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 89.0.4389.114

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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/2021/03/stable-channel-update-for-desktop_30.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2021-042/
https://exchange.xforce.ibmcloud.com/vulnerabilities/199172
https://exchange.xforce.ibmcloud.com/vulnerabilities/199171
https://exchange.xforce.ibmcloud.com/vulnerabilities/199173
https://exchange.xforce.ibmcloud.com/vulnerabilities/199174

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

Identifikátor

Apache Druid - bezpečnostná zraniteľnosť

Popis

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

Dátum prvého zverejnenia varovania

29.03.2021

CVE

CVE-2021-26919

Zasiahnuté systémy

Apache Druid vo verzii staršej ako 0.20.2

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://exchange.xforce.ibmcloud.com/vulnerabilities/198944
https://seclists.org/oss-sec/2021/q1/273
https://druid.apache.org/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware vRealize Operations Manager - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt vRealize Operations Manager, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

30.03.2021

CVE

CVE-2021-21975, CVE-2021-21983

Zasiahnuté systémy

vRealize Operations vo verzii staršej ako 7.5 Security Patch (82367)
vRealize Operations vo verzii staršej ako 8.0.1 Security Patch (83093)
vRealize Operations vo verzii staršej ako 8.1.1 Security Patch (83094)
vRealize Operations vo verzii staršej ako 8.2 Security Patch (83095)
vRealize Operations vo verzii staršej ako 8.3 Security Patch (83210)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom 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://www.bleepingcomputer.com/news/security/vmware-fixes-bug-allowing-attackers-to-steal-admin-credentials/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-vmware-vrealize-operations-manager-could-allow-for-remote-code-execution_2021-041/
https://exchange.xforce.ibmcloud.com/vulnerabilities/199104
https://exchange.xforce.ibmcloud.com/vulnerabilities/199105
https://www.vmware.com/security/advisories/VMSA-2021-0004.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.6**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ZTE ZXHN F623 produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť ZTE vydala bezpečnostnú aktualizáciu na svoj produkt ZXHN F623, ktorá opravuje bezpečnostnú zraniteľnosť.
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

29.03.2021

CVE

CVE-2021-21727

Zasiahnuté systémy

ZXHN F623 vo verzii staršej ako V6.0.0P3T34

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014744
https://exchange.xforce.ibmcloud.com/vulnerabilities/199107

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

Identifikátor

BuddyPress plugin pre WordPress - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu BuddyPress pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej HTTP požiadavky eskalovať svoje privilégiá, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

29.03.2021

CVE

CVE-2021-21389

Zasiahnuté systémy

BuddyPress vo verzii staršej ako 7.2.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Eskalácia privilégií

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nevyužívajú Wordpress plugin BuddyPress v zraniteľnej verzii. V prípade, že áno, 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/198913
https://github.com/buddypress/BuddyPress/security/advisories/GHSA-m6j4-8r7p-wpp3
https://wordpress.org/plugins/buddypress/

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

Identifikátor

SolarWinds Orion Virtual Infrastructure Monitor - bezpečnostná zraniteľnosť

Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na svoj produkt Orion Virtual Infrastructure Monitor, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.03.2021

CVE

CVE-2021-27277

Zasiahnuté systémy

Orion Virtual Infrastructure Monitor vo verzii staršej ako 2020.2.5

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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/199111
https://www.zerodayinitiative.com/advisories/ZDI-21-373/
https://documentation.solarwinds.com/en/Success_Center/SAM/Content/Release_Notes/SAM_2020-2-5_release_notes.htm

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

Identifikátor

ForgeRock OpenAM produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť ForgeRock vydala bezpečnostnú aktualizáciu na svoj produkt OpenAM, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

25.03.2021

CVE

CVE-2021-29156

Zasiahnuté systémy

ForgeRock OpenAM vo verzii staršej ako 13.5.1
ForgeRock OpenAM vo verzii staršej ako 14.0.0

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú OpenAM v zraniteľnej verzii. V prípade, že áno, 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/198802
https://bugster.forgerock.org/jira/browse/OPENAM-10135
https://www.forgerock.com/blog/tag/openam

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

Identifikátor

MicroSeven MYM71080i-B produkt - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu MicroSeven MYM71080i-B. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

30.03.2021

CVE

CVE-2021-29255

Zasiahnuté systémy

MicroSeven MYM71080i-B vo verzii staršej ako F2.0.20 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktializácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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/198950
https://cybergladius.com/cve-2021-29255-vulnerability-disclosure/
https://www.microseven.com/index.html

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

Identifikátor

Bosch Rexroth ActiveMover - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Bosch vydala bezpečnostnú aktualizáciu na svoj produkt Rexroth ActiveMover, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

31.03.2021

CVE

CVE-2021-20986, CVE-2021-20987

Zasiahnuté systémy

Rexroth ActiveMover vo verzii staršej ako 3.0.26.x

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://psirt.bosch.com/security-advisories/bosch-sa-282922.html
https://psirt.bosch.com/security-advisories/bosch-sa-637429.html

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

Identifikátor

cURL libcurl - bezpečnostná zraniteľnosť

Popis

Vývojári programu cURL vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej HTTP požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

31.03.2021

CVE

CVE-2021-22876

Zasiahnuté systémy

cURL libcurl vo verzii staršej ako 7.76.0

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúča uistiť sa, či Vaše aplikácie nevyužívajú knižnicu libcurl v zraniteľnej verzii. V prípade, že áno, administrátorom a používateľom 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/199186
https://curl.se/docs/CVE-2021-22876.html

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

Identifikátor

TP-Link produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť TP-Link vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

26.03.2021

CVE

CVE-2021-3275

Zasiahnuté systémy

TL-WA801ND vo verzii staršej ako 0.9.1_3.16_up_boot[170905-rel56404]
TL-WA801N vo verzii staršej ako 0.9.1_3.16_up_boot[200116-rel61815]
TL-WR802N vo verzii staršej ako 0.9.1_3.17_up_boot[200421-rel38950]
Archer-C3150 (všetky verzie - ukončená podpora)
TD-W9977 (všetky verzie - ukončená podpora)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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/198847
https://packetstormsecurity.com/files/161989
https://seclists.org/fulldisclosure/2021/Mar/67
https://packetstormsecurity.com/files/cve/CVE-2021-3275
https://www.tp-link.com/us/

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

Identifikátor

Microcosm bluemonday - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microcosm vydala bezpečnostnú aktualizáciu na svoj produkt bluemonday, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

27.03.2021

CVE

CVE-2021-29272

Zasiahnuté systémy

Microcosm bluemonday vo verzii staršej ako 1.0.5

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú na HTML sanitizáciu Microcosm bluemonday. V prípade, že áno, administrátorom a používateľom 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/198964
https://github.com/microcosm-cc/bluemonday/releases/tag/v1.0.5