Security Rabbits

Your Security Rabbits report for January 30, 2022

Hot topics

Nothing today

Twitter

frycos

Blog post published with my special guest Microsoft Exchange (CVE-2022-21969)

Jan Schaumann

Yikes, yesterday's Windows Patch Tuesday bundle was a doozy: - CVE-2022-21907: CVSS 9.8 HTTP Stack RCE - CVE-2022-21969, CVE-2022-21846, CVE-21855: 9.0 Exchange RCE - CVE-2022-21874: 7.8 Security Center RCE - CVE-2022-21893: 8.8 Rogue RDP RCE - CVE-2022-21840: 7.7 Office RCE

Abdelhamid Naceri

Over 3 months for a fix release CVE-2022-21919 Make it even worst than before

Rapid Safeguard

Searching for Deserialization Protection Bypasses in Microsoft Exchange (CVE-202221969) #infosec #cybersecurity

C:\SysWoW64\Lulztigre

CVE-202221969 : Searching for Deserialization Protection Bypasses in Microsoft Exchange

Luis Diago aka h3st4k3r

- CVE-2022-21836 - Vulnerabilidad de falsificacin de certificados de Windows. - CVE-2022-21839: seguimiento de eventos de Windows relacionado con la denegacin de servicio de la lista de control de acceso discrecional.

The Hacker News

Microsoft also resolved six zero-days as part of its #PatchTuesday update, 2 of which are an integration of third-party fixes concerning the open-source libraries curl and libarchive. CVE-2021-22947 CVE-2021-36976 CVE-2022-21836 CVE-2022-21839 CVE-2022-21874 CVE-2022-21919

Securityblog

Searching for Deserialization Protection Bypasses in Microsoft Exchange (CVE-202221969) | by frycos | Jan, 2022 | Medium

CVE Trends

Top 3 trending CVEs on Twitter Past 24 hrs: CVE-2022-21907: 3.4M (audience size) CVE-2022-21919: 893.6K CVE-2022-21849: 861.2K Past 7 days: CVE-2022-21907: 3.4M CVE-2021-42392: 3.3M CVE-2021-44228: 3.3M

MisaelBan

Searching for Deserialization Protection Bypasses in #Microsoft #Exchange CVE-202221969 #cybersecurity #infosec #hacking #pentesting @Microsoft

Huzeyfe NAL

MS Exchange kullanclar iin acil yama vakti! CVE-2022-21969

metisreginae

#CyberAlertHigh 8AITAZDW NVD 7.8 IMPACT:5.9 EXPLOIT:1.8 #CWE_269 #CPE_MICROSOFT #CVE_2022_21895 : Windows User Profile Service Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21919. | CVE-2022-21919 Twitter Alert |

News

Security Affairs

Expert releases PoC for CVE-2022-21882 Windows local privilege elevation issue

A researcher disclosed an exploit for a Windows local privilege elevation issue (CVE-2022-21882) that allows anyone to gain admin privileges in Windows 10. The security researchers RyeLv has publicly released an exploit for a Windows local privilege elevation flaw (CVE-2022-21882) that allows anyone to gain admin privileges in Windows 10. The Win32k elevation of privilege […] The post Expert releases PoC for CVE-2022-21882 Windows local privilege elevation issue appeared first on Security Affairs.

Cyware News - Latest Cyber News

Multi-Stage Phishing Campaign Leverages BYOD Concept to Target Organizations

According to Microsoft 365 Defender Threat Intelligence Team, the campaign took advantage of the devices that did not implement MultiFactor Authentication (MFA).

Security Affairs

Security Affairs newsletter Round 351

A new round of the weekly Security Affairs newsletter arrived! Every week the best security articles from Security Affairs free for you in your email box. If you want to also receive for free the newsletter with the international press subscribe here. QNAP force-installs update against the recent wave of DeadBolt ransomware infections US FCC bans […] The post Security Affairs newsletter

Security Affairs

Hybrid cloud campaign OiVaVoii targets company executives

A new hacking campaign, tracked as 'OiVaVoii', is targeting company executives with malicious OAuth apps. Researchers from Proofpoint have uncovered a new campaign named 'OiVaVoii' that is targeting company executives, former board members, Presidents and managers with bogus OAuth apps and cleverly-crafted lures sent from compromised Office 365 accounts. Microsoft has blocked many of the […] The post Hybrid cloud campaign OiVaVoii targets company executives appeared first on Security Affairs.

Security Affairs

Novel device registration trick enhances multi-stage phishing attacks

Microsoft has disclosed details of a large-scale phishing campaign using a novel device registration technique to target other enterprises. Microsoft has shared details of a large-scale phishing campaign that leverages stolen credentials to register devices on a target's network to extend the attack to other enterprises. The attack exploits the concept of bring-your-own-device (BYOD) by […] The post Novel device registration trick enhances multi-stage phishing attacks appeared first on Security Affairs.

Round 351 appeared first on Security Affairs.

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

Nothing today

Source: NIST

NIST CVE: Medium

Nothing today

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-22919

Adenza **AxiomSL** ControllerView through 10.8.1 allows **redirection** for SSO login URLs.

UNRATED | Vector: unkown | Created: 2022-01-30 | Updated: 2022-01-30

CVE-2022-24032

Adenza **AxiomSL** ControllerView through 10.8.1 is vulnerable to user enumeration. An attacker can identify valid usernames on the platform because a failed login attempt produces a different error message when the username is valid.

UNRATED | Vector: unkown | Created: 2022-01-30 | Updated: 2022-01-30

CVE-2022-0407

Heap-based Buffer Overflow in Conda vim prior to 8.2.

UNRATED | Vector: unkown | Created: 2022-01-30 | Updated: 2022-01-30

CVE-2022-0273

Improper Access Control in **Pypi** calibreweb prior to 0.6.16.

UNRATED | Vector: unkown | Created: 2022-01-30 | Updated: 2022-01-30

CVE-2022-0339

Server-Side Request Forgery (SSRF) in **Pypi** calibreweb prior to 0.6.16.

UNRATED | Vector: unkown | Created: 2022-01-30 | Updated: 2022-01-30

CVE-2021-46660

Signiant Manager+Agents before 15.1 allows XML External Entity (XXE) attacks.

UNRATED | Vector: unkown | Created: 2022-01-30 | Updated: 2022-01-30

CVE-2022-0408

Stack-based Buffer Overflow in Conda vim prior to 8.2.

UNRATED | Vector: unkown | Created: 2022-01-30 | Updated: 2022-01-30

CVE-2022-0413

Use After Free in Conda vim prior to 8.2.

UNRATED | Vector: unkown | Created: 2022-01-30 | Updated: 2022-01-30

Source: Hybrid Analysis

Top malicious files

100% Threat score	malwarefromv3rm . js
100% Threat score	Libes . exe
100% Threat score	challenge . exe
100% Threat score	npp . 8 . 2 . Installer . exe
100% Threat score	system32 . exe
100% Threat score	Pandoragg . dll
100% Threat score	bro . exe
100% Threat score	npp . 8 . 2 . Installer . exe
100% Threat score	FH5 TOOL BY DBZ . EXE
100% Threat score	avery . exe
100% Threat score	1 . WinRAR
100% Threat score	7C4FFE57E82CCCD99D334DAFE76578949030CD41A4D3BC2A4A37045689B4C9AD
100% Threat score	vanish . wtf . exe
92% Threat score	uxx3 . ocx

92%
Threat score
uxx2 . ocx

85%
Threat score
Antidetect_PPE_January2022_r4 . exe

74%
Threat score
Amap_V11 . 13 . 0 . 2925_android_C3060_(Build2201171717-64) . apk

71%
Threat score
cfx_rat . exe

Source: Hybrid Analysis

Top malicious URL

100%
Threat score
http://3rdbasela . com/

79%
Threat score
http://url6383 . of-shopping . com/ls/click?upn=YCoa4DE-2FdkA-2B-2BTjJqoelNcPpM6cf-2FmE7NaL4-2BZpydnp3aJy37pjVPdU8EvrmVlXJIRMSBVGtyqB2-2FQ0T4LG0wg-3D-3DPjJq_hBreS5cti-2FMkLgJWUlaYjJr1L-2FlGTUtefji74TcKHHXpWwZnWStULwFQtyKV9XLjsP2UL5o3rwO1kyjzJmskct3bsKMOii2Wv3UJ3TUqcHgoBEWobd0qzHau-2FBGVOOciU8c7tI6-2Foy4YJBCpM3EodmX3-2B-2B-2Bp3naUFeXLeX-2BUZ1vDWhb7sz4RMeBkiFyISAUQzJruCzJtwXkMPKHmllAlfhb828Vx3TN-2B80y7Ci7VOgI-3D

79%
Threat score
https://nx . tn/JjKmv

77%
Threat score
http://www . 3rdbasela . com/

Source: SpamHaus

Top spamming countries

#1 United States of America

#2 China

#3 Russian Federation

#4 Mexico

#5 Dominican Republic

#6 India

#7 Saudi Arabia

#8 Japan

#9 Brazil

#10 Korea, Republic of

Source: SpamHaus

Top spammers

#1 **Canadian Pharmacy**
A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.

#2 **PredictLabs / Sphere Digital**
This operation uses dozens of "hosting" companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco.

#3 **Hosting Response / Michael Boehm**
Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.

#4 **Mint Global Marketing / Adgenics / Cabo Networks**
Florida affiliate spammers and bulletproof spam hosters

#5 **RetroCubes**
Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.

#6 **Michael Persaud**
Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.

#7 **Cyber World Internet Services/ e-Insites**
Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe.

#8 **RR Media**
A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.

#9 **Kobeni Solutions**
High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US FTC in 2014.

Source: SpamHaus

Top countries with botnet

- #1 China
- #2 India
- #3 Thailand
- #4 Indonesia
- #5 Viet Nam
- #6 United States of America
- #7 Algeria
- #8 Brazil
- #9 Pakistan
- #10 Iran (Islamic Republic of)

Source: SpamHaus

Top phishing countries

- #1 United States
- #2 Germany
- #3 Netherlands
- #4 Russia
- #5 India
- #6 Singapore
- #7 France
- #8 Ireland
- #9 Canada
- #10 Japan