



Your Security Rabbits report for February 05, 2022

Hot topics

Nothing today

News



Security
Affairs

[CISA orders federal agencies to fix actively exploited CVE-2022-21882 Windows flaw](#)
US CISA ordered federal agencies to patch their systems against actively exploited CVE-2022-21882 Windows flaw. The Cybersecurity and Infrastructure Security Agency (CISA) has ordered federal agencies to address their systems against an actively exploited Windows vulnerability tracked as CVE-2022-21882. "CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence that threat [...] The post CISA orders federal agencies to fix actively exploited CVE-2022-21882 Windows flaw appeared first on Security Affairs.



Security
Affairs

[FBI issued a flash alert on Lockbit ransomware operation](#)

The FBI released a flash alert containing technical details associated with the LockBit ransomware operation. The Federal Bureau of Investigation (FBI) has issued a flash alert containing technical details and indicators of compromise associated with LockBit ransomware operations. The LockBit ransomware gang has been active since September 2019, in June 2021 the group announced the LockBit 2.0 RaaS. Like [...] The post FBI issued a flash alert on Lockbit ransomware operation appeared first on Security Affairs.



Security
Affairs

[LockBit ransomware gang claims to have stolen data from PayBito crypto exchange](#)

LockBit ransomware gang claims to have stolen customers' data from the PayBito crypto exchange. PayBito is a bitcoin and cryptocurrency exchange for major cryptocurrencies including Bitcoin Cash, Bitcoin, Ethereum, HXC, Litecoin, Ethereum Classic. The exchange is operated by global blockchain and IT services company HashCash. LockBit ransomware operators claim to have stolen customers' data from the PayBito crypto exchange, [...] The post LockBit ransomware gang claims to have stolen data from PayBito crypto exchange appeared first on Security Affairs.



The Hacker
News

[Microsoft Uncovers New Details of Russian Hacking Campaign Targeting Ukraine](#)

Microsoft on Friday shared more of the tactics, techniques, and procedures (TTPs) adopted by the Russia-based Gamaredon hacking group to facilitate a barrage of cyber espionage attacks aimed at several entities in Ukraine over the past six months. The attacks are said to have singled out government, military, non-government organizations (NGO), judiciary, law enforcement, and non-profit

Twitter



huntr
Hacktivity

null in (CVE-2022-0443) reported by alkyne - Patch: [#bugbounty](#) [#infosec](#) [#opensource](#)



Open
Source
CVEs

(CVE-2022-0443): Use After Free in vim/vim. Disclosed by , fixed by vim maintainers... [#opensource](#) [#CVE](#) [#bugbounty](#) [#security](#) [#vulnerability](#)











Robo

Potentially Critical CVE Detected! CVE-2022-0443 Description: Use After Free in Conda vim prior to 8.2.... CVSS: 8.62 [#CVE](#) [#CyberSecurity](#)



IBM Security Verify Access privilege escalation | CVE-2021-39070 -

Shadow Alerts	#DataBreach	RedPacket Security	
 RedPacket Security	Vim code execution CVE-2022-0443 -	 Remotely Alerts	Severity: Use After Free in Conda vim prior to 8.2... CVE-2022-0443 Link for more:
 SRM IT Risk	IT Risk: HPE.ArubaOS-CX 8000 -2/3 CVE-2021-41839 CVE-2020-27339 CVE-2021-33626 CVE-2021-33627 CVE-2021-418 CVE-2021-418 CVE-2021-41837 CVE-2021-43323 CVE-2021-42554 CVE-2021-33625 CVE-2021-43522 CVE-2021-42113 CVE-2021-42113	 SRM IT Risk	IT Risk: HPE.Multiple Vulnerabilities in ArubaOS-CX 8000 Series Switches -2/3 CVE:CVE-2020-5953 CVE-2021-41610 CVE-2021-41840 CVE-2021-41841 CVE-2021-41839 CVE-2020-27339 CVE-2021-33626 CVE-2021-33627 CVE-2021-418 CVE-2021-418 CVE-2021-41837 CVE-2021-43323 CVE-2021-42554
 SRM IT Risk	IT Risk: Multiple Vulnerabilities in HPE.Aruba 9000 -2/2 CVE-2021-41610 CVE-2021-41840 CVE-2021-41839 CVE-2020-27339 CVE-2021-33626 CVE-2021-33627 CVE-2021-41838 CVE-2021-41837 CVE-2021-43323 CVE-2021-42554 CVE-2021-33625 CVE-2021-43522 CVE-2021-42113 CVE-2021-42059	 www.sesin.at	New post from (CVE-2021-39070 (security_verify_access, security_verify_access_docker)) has been published on
 Wolfgang Sesin	New post from (CVE-2021-39070 (security_verify_access, security_verify_access_docker)) has been published on	 Remotely Alerts	Severity: IBM Security Verify Access 10.0.0.0, 10.... CVE-2021-39070 Link for more:

Source: *NIST*

NIST CVE: Critical

CVE-2022-24218	An issue in /admin/delete_image.php of eliteCMS v1.0 allows attackers to delete arbitrary files. <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-05</div> </div>	CVE-2022-24223	AtomCMS v2.0 was discovered to contain a SQL injection vulnerability via /admin/login.php. <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-05</div> </div>
CVE-2021-39070	IBM Security Verify Access 10.0.0.0, 10.0.1.0 and 10.0.2.0 with the advanced access control authentication service enabled could allow an attacker to authenticate as any user on the system. IBM X-Force ID: 215353. <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-02</div> <div>Updated: 2022-02-05</div> </div>	CVE-2021-42554	SMM memory corruption vulnerability allowing a possible attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM. <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-03</div> <div>Updated: 2022-02-05</div> </div>
CVE-2022-0443	Use After Free in Conda vim prior to 8.2. <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-02</div> <div>Updated: 2022-02-05</div> </div>		

Source: *NIST*

NIST CVE: High

CVE-2022-0417	Heap-based Buffer Overflow in Conda vim prior to 8.2. <div> <div>HIGH</div> <div>Vector: local</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-05</div> </div>	CVE-2021-39066	IBM Financial Transaction Manager 3.2.4 does not invalidate session any existing session identifier gives an attacker the opportunity to steal authenticated sessions. IBM X-Force ID: 215040. <div> <div></div> <div></div> <div></div> <div></div> </div>
---------------	---	----------------	--

CVE-2021-39044

IBM Financial Transaction Manager 3.2.4 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 214210.

HIGH Vector: Created: Updated:
network 2022-02-02 2022-02-05

CVE-2022-22509

In **Phoenix** Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows a low privileged user to enable full access to the device configuration.

HIGH Vector: Created: Updated:
network 2022-02-02 2022-02-05

CVE-2022-24122

kernel/ucount.c in the **Linux** kernel 5.14 through 5.16.4, when unprivileged user namespaces are enabled, allows a use-after-free and privilege escalation because a ucounts object can outlive its namespace.

HIGH Vector: Created: Updated:
local 2022-01-29 2022-02-05

CVE-2022-23601

Symfony is a PHP framework for web and console applications and a set of reusable PHP components. The Symfony form component provides a CSRF protection mechanism by using a random token injected in the form and using the session to store and control the token submitted by the user. When using the FrameworkBundle, this protection can be enabled or disabled with the configuration. If the configuration is not specified, by default, the mechanism is enabled as long as the session is enabled. In a recent change in the way the configuration is loaded, the default behavior has been dropped and, as a result, the CSRF protection is not enabled in form when not explicitly enabled, which makes the application sensible to CSRF attacks. This issue has been resolved in the patch versions listed and users are advised to update. There are no known workarounds for this issue.

HIGH Vector: Created: Updated:
network 2022-02-01 2022-02-05

Source: *NIST*

NIST CVE: Medium

CVE-2021-44451

Apache Superset up to and including 1.3.2 allowed for registered database connections password leak for authenticated users. This information could be accessed in a non-trivial way. Users should upgrade to Apache Superset 1.4.0 or higher.

MEDIUM Vector: Created: Updated:
network 2022-02-01 2022-02-05

CVE-2022-24301

In Minetest before 5.4.0, players can add or subtract items from a different player's **inventory**.

MEDIUM Vector: Created: Updated:
network 2022-02-02 2022-02-05

CVE-2021-38560

Ivanti Service Manager 2021.1 allows reflected XSS via the appName parameter associated with ConfigDB calls, such as in RelocateAttachments.aspx.

MEDIUM Vector: Created: Updated:
network 2022-02-01 2022-02-05

CVE-2022-0432

Prototype Pollution in **GitHub** repository mastodon/mastodon prior to 3.5.0.

MEDIUM Vector: Created: Updated:
network 2022-02-02 2022-02-05

CVE-2021-42059

Stack overflow vulnerability that allows a local root user to access UEFI DXE driver and execute arbitrary code.

MEDIUM Vector: Created: Updated:
local 2022-02-03 2022-02-05

Source: *NIST*

NIST CVE: Low

Nothing today

Source: *NIST*

NIST CVE: Unrated

CVE-2022-0437	Cross-site Scripting (XSS) - DOM in NPM karma prior to 6.3.14. <div>UNRATEDVector: unknwnCreated: 2022-02-05Updated: 2022-02-05</div>	CVE-2022-0501	Cross-site Scripting (XSS) - Reflected in Packagist ptrofimov/beanstalk_console prior to 1.7.12. <div>UNRATEDVector: unkownCreated: 2022-02-05Updated: 2022-02-05</div>
CVE-2021-38172	perM 0.4.0 has a Buffer Overflow related to strncpy. (Debian initially fixed this in 0.4.0-7.) <div>UNRATEDVector: unknwnCreated: 2022-02-05Updated: 2022-02-05</div>		

Source: *Hybrid Analysis*

Top malicious files

100% Threat score	Orion v1 (.) 3 (.) exe	100% Threat score	copy-text-on-screen-pro[dlandroid (.) com] (.) apk
100% Threat score	Dying Light 2 Stay Human Trainer Setup (.) exe	100% Threat score	Setup (.) exe
100% Threat score	Vonex-Fortnite (.) exe	100% Threat score	tmpwzffbiqy
100% Threat score	Capture Boss (.) exe	100% Threat score	Iron Sea - Frontier Defenders (.) exe
100% Threat score	Comet_Space_Designer (.) exe	100% Threat score	wendys-wellness (.) exe
100% Threat score	K_Game_v2 (.) 23 (.) exe	87% Threat score	3a680c8620adcad22a0606eb8411d2f45fcd5488e122dba75c9a109aa8de11b7 (.) exe
80% Threat score	sEraser (.) exe	80% Threat score	Video Cut Magic Music_apkpure (.) com (.) apk
77% Threat score	Comet (.) exe	75% Threat score	1 (.) Rummage (.) exe
72% Threat score	setting (.) exe		





Top malicious URL

100% Threat score	https://spitvelvet(.)top/gloria/tb(.)php?t=16439471381643947524519	90% Threat score	http://forms(.)gle/j7oFBQUPEG3Fi4mL7
90% Threat score	http://metamask(.)io/	86% Threat score	https://www(.)partha(.)com/downloads/GIMP/GIMP-2(.)10(.)22-64bit(.)exe
82% Threat score	http://un-org(.)yupage(.)com/test2/serverok(.)html	77% Threat score	http://maxkarson(.)com/that-apology-you-wanted
74% Threat score	http://preventiontrainingservices(.)com/	74% Threat score	https://minimore(.)com/b/rurQ9/1
71% Threat score	http://www(.)securityupdated(.)com/b/builder1(.)exe		

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

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



#3 Thailand



#5 United States of America



#7 Brazil



#9 Pakistan



#2 India



#4 Indonesia



#6 Algeria



#8 Viet Nam



#10 Iran (Islamic Republic of)

Source: [SpamHaus](#)

Top phishing countries



#1 United States



#3 France



#5 Russia



#7 Netherlands



#9 Bulgaria



#2 India



#4 Germany



#6 Hong Kong



#8 Australia



#10 Singapore

