




Your Security Rabbits report for February 06, 2022


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

Hot topics

PwnKit.

pkexec (PolKit or Policy Kit) allows an authorized user to execute a program as another user on many Linux distributions. `br>`

A flaw has been discovered in November 2021. It allowed standard user accounts to gain root privileges.

The flaw, called PwnKit (CVE-2021-4034) was patched on January 25th.

This is a gentle reminder that you should patch your Linux systems as well. :)

--

JL Dupont

News



Security

Argo CD flaw could allow stealing sensitive data from Kubernetes Apps
A flaw in Argo CD tool for Kubernetes could



Security

Israeli surveillance firm QuaDream emerges from the dark

One of the Apple iOS zero-day flaws exploited by the NSO group was also used by another

be exploited by attackers to steal sensitive data from Kubernetes Apps. A zero-day vulnerability, tracked as CVE-2022-24348, in the Argo CD tool for Kubernetes could be exploited by attackers to steal sensitive data from Kubernetes Apps, including passwords and API keys. The flaw received a CVSS [...] The post Argo CD flaw could allow stealing sensitive data from Kubernetes Apps appeared first on Security Affairs.

surveillance firm named QuaDream. One of the vulnerabilities in Apple iOS that was previously exploited by the spyware developed by the Israeli company NSO Group was also separately used by another surveillance firm named QuaDream. Like NSO Group, QuaDream develops [...] The post Israeli surveillance firm QuaDream emerges from the dark appeared first on Security Affairs.

New Argo CD Bug Could Let Hackers Steal Secret Info from Kubernetes Apps
Users of the Argo continuous deployment (CD) tool for Kubernetes are being urged to push through updates after a zero-day vulnerability was found that could allow an attacker to extract sensitive information such as passwords and API keys. The flaw, tagged as CVE-2022-24348 (CVSS score: 7.7), affects all versions and has been addressed in versions 2.3.0, 2.2.4, and 2.1.9. Cloud security firm



Security Affairs newsletter Round 352
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. LockBit ransomware gang claims to have stolen data from PayBito crypto exchange FBI issued [...] The post Security Affairs newsletter Round 352 appeared first on Security Affairs.

Source: [NIST](#)

NIST CVE: Critical

Nothing today

Source: [NIST](#)

NIST CVE: High

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: local

Created: 2022-01-29

Updated: 2022-02-06

Source: [NIST](#)

NIST CVE: Medium

Nothing today

Source: [NIST](#)

NIST CVE: Low

Nothing today

Source: [NIST](#)

NIST CVE: Unrated

CVE-2022-22831

An issue was discovered in Servisnet Tessa 0.0.2. An attacker can add a new sysadmin user via a manipulation of the Authorization HTTP header.

UNRATED

Vector: Created: Updated:
unknown 2022- 2022-02-
02-06 06

CVE-2022-22833

An issue was discovered in Servisnet Tessa 0.0.2. An attacker can obtain sensitive information via a /js/app.js request.

UNRATED

Vector: Created: Updated:
unknown 2022- 2022-02-
02-06 06

CVE-2022-22832

An issue was discovered in Servisnet Tessa 0.0.2. Authorization data is available via an unauthenticated /data-service/users/ request.

UNRATED

Vector: Created: Updated:
unknown 2022- 2022-02-
02-06 06

CVE-2021-39280

Certain **Korenix** JetWave devices allow authenticated users to execute arbitrary code as root via /syscmd.asp. This affects 2212X before 1.9.1, 2212S before 1.9.1, 2212G before 1.8, 3220 V3 before 1.5.1, 3420 V3 before 1.5.1, and 2311 through 2022-01-31.

UNRATED

Vector: Created: Updated:
unknown 2022- 2022-02-
02-06 06

CVE-2021-41816

CGI.escape_html in **Ruby** before 2.7.5 and 3.x before 3.0.3 has an integer overflow and resultant buffer overflow via a long string on platforms (such as Windows) where size_t and long have different **numbers** of bytes. This also affects the CGI gem before 0.3.1 for Ruby.

UNRATED

Vector: Created: Updated:
unknown 2022- 2022-02-
02-06 06

CVE-2022-0502

Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.

UNRATED

Vector: Created: Updated:
unknown 2022-02- 2022-02-
06 06

CVE-2022-23206

In **Apache Traffic Control** Traffic Ops prior to 6.1.0 or 5.1.6, an unprivileged user who can reach Traffic Ops over HTTPS can send a specially-crafted POST request to /user/login/oauth to **scan** a port of a server that Traffic Ops can reach.

UNRATED

Vector: Created: Updated:
unknown 2022- 2022-02-
02-06 06

CVE-2007-20001

StarWind **iSCSI** SAN before 3.5 build 2007-08-09 allows **socket** exhaustion.

UNRATED

Vector: Created: Updated:
unknown 2022- 2022-02-
02-06 06

CVE-2013-20004

StarWind **iSCSI** SAN before 6.0 build 2013-03-20 allows a memory leak.

UNRATED

Vector: Created: Updated:
unknown 2022- 2022-02-
02-06 06

CVE-2022-24552

StarWind SAN and NAS before 0.2 build 1685 allows remote code execution via a virtual disk management command.

UNRATED

Vector: Created: Updated:
unknown 2022- 2022-02-
02-06 06

CVE-2022-24551

StarWind SAN and NAS before 0.2 build 1685 allows users to reset other users' passwords.

UNRATED










Vector: Created: Updated:
unknown 2022- 2022-02-
02-06 06

Top malicious files

100% Threat score	2022-02-04_1118 (.) xls	100% Threat score	CuteWriter (.) exe
100% Threat score	youareanidiotvirus (.) exe	100% Threat score	Setup (.) exe
100% Threat score	hidemyname (.) exe	100% Threat score	ktootkryltotsinmorgenshterna (.) exe
100% Threat score	fvfdgb (.) exe	81% Threat score	kodit (.) co (.) kr (.) htm
75% Threat score	setup (.) exe		











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

Source: SpamHaus

Top phishing countries

	#1 United States		#2 Germany
	#3 Netherlands		#4 France
	#5 India		#6 Hong Kong
	#7 Russia		#8 Singapore
	#9 United Kingdom		#10 Indonesia

Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://119(.)102(.)177(.)162:51778/i	100% Threat score	http://113(.)92(.)158(.)128:54667/Mozi(.)m
100% Threat score	http://115(.)52(.)178(.)126:58259/Mozi(.)m	100% Threat score	http://125(.)41(.)14(.)212:47180/Mozi(.)m
100% Threat score	http://117(.)201(.)207(.)170:54907/Mozi(.)m	100% Threat score	http://42(.)224(.)250(.)37:50187/Mozi(.)m
100%	http://117(.)215(.)213(.)200:33737/Mozi	100%	http://218(.)104(.)175(.)23:39185/Mozi(.)

Threat score	(.) m
100% Threat score	http://124(.) 92(.) 1(.) 243:59301/bin(.) sh
77% Threat score	http://www(.) encipher(.) com/
74% Threat score	https://help(.) venmo(.) com/hc/en-us/articles/4414673650579
72% Threat score	http://yogagympornvideos(.) com/thumbbrw(.) php?utm_source=65e8196&utm_content=d6d

Threat score	a
95% Threat score	http://js(.) users(.) 51(.) la/19013103(.) js
77% Threat score	http://orthoteers(.) com/
72% Threat score	http://disctk(.) xyz/