Your Security Rabbits report for March 03, 2022

Source: Ransom Watch

Ransomware attacks

conti	Target: Buhck Gruppe(2022-03-03)	conti	Target: GRUPPO ANGELANTONI(2022-03-03)
conti	Target: Sport Vision(2022-03-03)	lockbit2	Target: sapulpaps . org(2022-03-03)
clop	Target: MCH-GROUP . COM (2022-03-02)	lockbit2	Target: www . wimmog . ch(2022-03-02)
lockbit2	Target: www . tccm . com(2022-03-02)	lockbit2	Target: www . haeny . com(2022-03-02)
lockbit2	Target: www . elitecorp . c . . . (2022-03-02)	lockbit2	Target: wimmog . ch(2022-03-02)
lockbit2	Target: tccm . com(2022-03-02)	clop	Target: SSMSJUSTICE . COM (2022-03-02)
clop	Target: SLIMSTOCK . COM (2022-03-02)	clop	Target: MTMRECOGNITION . COM (2022-03-02)
clop	Target: ALEXIM . COM (2022-03-02)	clop	Target: JCWHITE . COM (2022-03-02)
clop	Target: JBINSTANTLAWN . NET (2022-03-02)	conti	Target: HOL-MAC Corp . (2022-03-02)
lockbit2	Target: haeny . com(2022-03-02)	lockbit2	Target: elitecorp . com(2022-03-02)
clop	Target: EDAN . COM (2022-03-02)	clop	Target: DUTTONFIRM . COM (2022-03-02)
clop	Target: CAPCARPET . COM (2022-03-02)	clop	Target: BOLTONUSA . COM (2022-03-02)

Hot topics

Ransomware threat intelligence

Security Rabbits will now report DDOS statistics.

News

Security Affairs

A cyberattack on Russian satellites is an act of war, the invasion of Ukraine no

Russia considers it legitimate to invade another country but warns it will consider cyberattacks on its satellites an act of war. Anonymous and the numerous hacker groups that declared war on Russia continue to target Russian government entities and private businesses. Yesterday, the hacking group Network Battalion 65 ('NB65') which is affiliated with Anonymous, announced to have [...] The post A cyberattack on Russian satellites is an act of war, the invasion of Ukraine no appeared first on Security Affairs.

Security Affairs

Anonymous and its affiliates continue to cause damage to Russia

The massive operation launched by the Anonymous collective against Russia for its illegitimate invasion continues. The popular collective Anonymous, and its affiliates, relentlessly continue their offensive against Russian targets. In the last few hours, in addition to government sites, the sites of the country's main banks have been brought to their knees. News of alleged [...] The post Anonymous and its affiliates continue to cause damage to Russia appeared first on Security Affairs.

Security Affairs

Asylum Ambuscade spear-phishing campaign targets EU countries aiding Ukrainian refugees

A spear-phishing campaign, tracked as Asylum Ambuscade, targets European government personnel aiding Ukrainian refugees. Researchers from cybersecurity firm Proofpoint uncovered a spear-phishing campaign, likely conducted by a nation-state actor, that compromised a Ukrainian armed service member's email account to target European government personnel involved in managing the logistics of refugees fleeing Ukraine. The phishing messages [...] The post Asylum Ambuscade spear-phishing campaign targets EU countries aiding Ukrainian refugees appeared first on Security Affairs.

Cyware News - Latest Cyber News

Bad actors are becoming more successful at evading AI/ML technologies

One of the takeaways from a new research on 2021 threat trends is that hackers are getting more successful at evading AI/ML technologies, prompting firms to redouble efforts in the innovation race.

Cyware News - Latest Cyber News

Beware of WhisperGate and HermeticWiper - Warns the FBI and CISA

The FBI and CISA issued a joint advisory regarding the WhisperGate and HermeticWiper malware. These malware strains are being used to target organizations located in Ukraine. In January 2022, Ukraine was targeted by the destructive WhisperGate malware, pretending to be a ransomware.Soon after that, HermeticWiper was deployed in conjunction with HermeticRansom decoys to render devices unbootable.

Threatpost

Conti Ransomware Decryptor, TrickBot Source Code Leaked

The decryptor spilled by ContiLeaks won't work with recent victims. Conti couldn't care less: It's still operating just fine. Still, the dump is a bouquet's worth of intel.

Krebs on Security

Conti Ransomware Group Diaries, Part II: The Office

Earlier this week, a Ukrainian security researcher leaked almost two years' worth of internal chat logs from Conti, one of the more rapacious and ruthless ransomware gangs in operation today. Tuesday's story examined how Conti dealt with its own internal breaches and attacks from private security firms and governments. In Part II of this series we'll explore what it's like to work for Conti, as described by the Conti employees themselves.

IT Security Guru

Cyberattacks in Ukraine could reach other countries

While the majority of cyberattacks in Ukraine are planned and highly targeted, there are signs that things are set to change. A new Trojan dubbed "FoxBlade" was discovered by Microsoft researchers on Ukrainian government systems that would allow attackers to use infected PCs in DDoS attacks. Experts are concerned that malware operators will try to infect [...] The post Cyberattacks in Ukraine could reach other countries appeared first on IT Security Guru.

Cyware News - Latest Cyber News

DanaBot Launches DDoS Attack Against the Ukrainian Ministry of Defense

The DDoS attack was launched against the Ukrainian Ministry of Defense's webmail server by leveraging DanaBot to deliver a second-stage malware payload using the download and execute command.

Cyware News - Latest Cyber News

Data Wiper Malware Wreak Havoc on Ukrainian Organizations

Lately, researchers at ESET uncovered a third new data wiper, dubbed IssacWiper, that was used against hundreds of machines. Previously, HermeticWiper and WhisperGate malware were already seen targeting Ukrainian firms. According to the researchers, the malware has been active since February 24 and includes both a wiper and a worm component to spread HermeticWiper in local networks.

Cyware News - Latest Cyber News

Google expands security protections for Ukrainian users

Google announced on Tuesday that it was increasing security measures to help protect Ukrainian civilians and websites, following similar moves by other technology giants in recent days.

The Hacker News

Hackers Try to Target European Officials to Get Info on Ukrainian Refugees, Supplies

Details of a new nation-state sponsored phishing campaign have been uncovered setting its sights on European governmental entities in what's seen as an attempt to obtain intelligence on refugee and supply movement in the region. Enterprise security company Proofpoint, which detected the malicious emails for the first time on February 24, 2022, dubbed the social engineering attacks "Asylum

The Hacker News

Hackers Who Broke Into NVIDIA's Network Leak DLSS Source Code Online

American chipmaking company NVIDIA on Tuesday confirmed that its network was breached as a result of a cyber attack, enabling the perpetrators to gain access to sensitive data, including source code purportedly associated with its Deep Learning Super Sampling (DLSS) technology. "We have no evidence of ransomware being deployed on the NVIDIA environment or that this is related to the

Blog â€“ Flashpoint

How Telegram Became a Critical Source of Intelligence in the Ukraine-Russia War

Telegram comes of age Telegram was created in 2013 by Pavel Durov, a Russian tech entrepreneur who has, to a large extent, managed to withstand pressure from Russian authorities and keep Telegram free and clear of oversight. This remains the key to Telegram's power today: it's a viable communications alternative to social platforms that are [...] The post How Telegram Became a Critical Source of Intelligence in the Ukraine-Russia War appeared first on Flashpoint.

Cyware News -

Iranian Hackers Introduce New Malware to Target Middle East

Mandiant tracked cybercriminals collaborating under the moniker UNC3313 deploying two new targeted malware to claim victims in the middle east. The group

IT Security Guru

Medical infusion pumps vulnerable to attack

Researchers at Palo Alto Networks have collected data from 200,000 medical infusion pumps used to administer medicines and fluids to patients, finding that 75% of them are running with known security

Latest Cyber News

moves quickly to gain remote access by using ScreenConnect to intrude systems within an hour of initial compromise. Furthermore, the security firm has also provided YARA rules to identify malware patterns.

Cyware News - Latest Cyber News

MuddyWater Rounds up its Arsenal with Multi-Malware Sets

Cybersecurity agencies released a joint cybersecurity advisory detailing malicious cyber operations by MuddyWater, which has been targeting a wide range of government and private-sector organizations in Asia, Africa, Europe, and North America. Among others, the CISA recommends organizations to use multi-factor authentication on a priority.

Security Affairs

NVIDIA discloses data breach after the recent ransomware attack

Chipmaker giant Nvidia confirmed a data breach after the recently disclosed security incident, proprietary information stolen. The chipmaker giant Nvidia was recentty victim of a ransomware attack that impacted some of its systems for two days. The security breach is not connected to the ongoing crisis in Ukraine, according to a person familiar with the [...] The post NVIDIA discloses data breach after the recent ransomware attack appeared first on Security Affairs.

Security Affairs

Popular open-source PJSIP library is affected by critical flaws

Researchers from JFrog's Security Research team discovered five vulnerabilities in the PJSIP open-source multimedia communication library.
Researchers from JFrog's Security Research team discovered five vulnerabilities in the popular PJSIP open-source multimedia communication library. PJSIP is a communication library written in C language implementing standard-based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. It [...] The post Popular open-source PJSIP library is affected by critical flaws appeared first on Security Affairs.

Naked Security

Ransomware with a difference: "Derestrict your software, or else!"

"Change your code to improve cryptomining"... or we'll dump 1TB of stolen secrets.

The Hacker News

Report: Nearly 75% of Infusion Pumps Affected by Severe Vulnerabilities

An analysis of data crowdsourced from more than 200,000 network-connected infusion pumps used in hospitals and healthcare entities has revealed that 75% of those medical devices contain security weaknesses that could put them at risk of potential exploitation. "These shortcomings included exposure to one or more of some 40 known cybersecurity vulnerabilities and/or alerts that they had one or

IT Security Guru

Salt Security releases State of API Security Report

Salt Security released its Salt Labs State of API Security Report, Q1 2022. The bi-annual report found that 95% of surveyed organisations have experienced an API security incident in the past 12 months. The research showed that 34% of respondents - all of whom are running production APIs - lack any kind of API security [...] The post Salt Security releases State

issues. Research has revealed that tens of thousands of devices are vulnerable to six critical severity flaws (9.8 out of 10) reported in 2019 [...] The post Medical infusion pumps vulnerable to attack appeared first on IT Security Guru.

CyberScoop

NATO countries' refugee management may have been targeted by Belarus-linked hackers

A hacking group with a history of phishing attacks and disinformation against NATO nations may be using compromised Ukrainian armed service member emails to target European officials tasked with managing logistics around refugees fleeing Ukraine, according to findings published Monday. Researchers with cybersecurity firm Proofpoint report they detected an email Feb. 24 that carried a subject referencing the Feb. 24 emergency meeting of NATO on the day the Russian government began its military attack on Ukraine. The email included an attached Microsoft Excel spreadsheet titled "list of persons.xlsx" that the researchers later determined included malware that, if installed, sought to gather in[...]

Cyware News - Latest Cyber News

Over 100,000 medical infusion pumps vulnerable to years old critical bug

The most prevalent critical-severity flaw encountered is CVE-2019-12255, a memory corruption bug in the VxWorks real-time operating system used for embedded devices, including infusion pump systems.

CyberScoop

Proposal for industries to report big cyberattacks, ransomware payments wins Senate approval

The Senate passed legislation Tuesday evening requiring critical infrastructure owners to report to the feds when they suffer a major cyberattack or make a ransomware payment -- shaking loose a bill that got stuck in the chamber last year. Under the measure, which now moves to the House for potential consideration, those critical infrastructure owners and operators as well as federal agencies would have to disclose a significant incident to the Department of Homeland Security's Cybersecurity and Infrastructure Agency within 72 hours. The same owners and operators would have to report any ransomware payments to CISA, too, only within 24 hours. Its intent is to give CISA the information it nee[...]

Threatpost

RCE Bugs in Hugely Popular VoIP Apps: Patch Now!

The flaws are in the ubiquitous open-source PJSIP multimedia communication library, used by the Asterisk PBX toolkit that's found in a massive number of VoIP implementations.

Cyware News - Latest Cyber News

Russian space agency says hacking satellites is an act of war

Dmitry Rogozin, the current head of the Russian Roscosmos State Space Corporation, added that such attempts would also be considered crimes and investigated by Russia's law enforcement agencies.

IT Security Guru

TeaBot malware resurfaces on Google Play Store

TeaBot malware has been spotted on the Google Play Store posing as a QR code app, already spreading to more than 10,000 devices. Its distributors used this trick in January, and while Google ousted those entries the malware has found its way back onto the Android repository. Cleafy, an online fraud management and prevention company, [...] The post TeaBot malware

of API Security Report appeared first on IT Security Guru.

resurfaces on Google Play Store appeared first on IT Security Guru.

Cyware News - Latest Cyber News

TeaBot Spreads via Google Play, Again!

Cleafy discovered the trojan disguised as a QR code app on Google Play Store, which has already spread to more than 10,000 devices. This is not the first time that TeaBot has propagated via the Play Store.

Threatpost

TeaBot Trojan Haunts Google Play Store, Again

Malicious Google Play apps have circumvented censorship by hiding trojans in software updates.

Cyware News - Latest Cyber News

Threat groups with Russian ties, malware used in Ukraine prompts alert for US health sector

An alert from The Department of Health and Human Services Cybersecurity Coordination Center warned about wiper malware and attacks from threat groups with ties to Russia amidst the ongoing conflict.

Cyware News - Latest Cyber News

TrickBot's AnchorDNS is Now Upgraded to AnchorMail

Researchers identified an improved version of the AnchorDNS backdoor, dubbed AnchorMail, being used in Conti ransomware attacks. Post-execution, AnchorMail creates a scheduled task for persistence that runs every 10 minutes. Experts recommend training your employees to spot phishing emails is also a part of an effective strategy.

The Hacker News

U.S. Senate Passes Cybersecurity Bill to Strengthen Critical Infrastructure Security

The U.S. Senate unanimously passed the "Strengthening American Cybersecurity Act" on Tuesday in an attempt to bolster the cybersecurity of critical infrastructure owners in the country. The new bipartisan legislation, among other things, stipulates entities that experience a cyber incident to report the attacks within 72 hours to the U.S. Cybersecurity and Infrastructure Security Agency (CISA),

ZDNet | security RSS

Ukraine calls for corporate support as Oracle suspends Russian operations

Updated: Mykhailo Fedorov requests the severance of business relationships with Russia. Oracle and SAP have taken this step.

CyberScoop

Ukraine conflict spurs questions of how to define cyberwar

Legal scholars and cybersecurity experts are closely watching events in Ukraine with an eye on how the Russian invasion may redefine the laws of war for the cyber era. Many agree that Ukraine's conflict with Russia -- an established cyber superpower that isn't hesitant about flexing its muscle aggressively -- could test the rules of war in new and unexpected ways. Some say it already has. Exactly how these rules might be redefined is the subject of significant debate. In recent days, authorities as disparate as the president of Microsoft and the chairman of the Senate Intelligence Committee have weighed in on how NATO's Article 5 provision for "collective defense," the Geneva Convention's pr[...]

Cyware News - Latest Cyber News

Ukrainian sites saw a 10x increase in attacks when invasion started

Internet security companies have recorded a massive wave of attacks against Ukrainian WordPress sites since Russia invaded Ukraine, aiming to take down the websites and cause general demoralization.

Cyware News - Latest Cyber News

Update: NVIDIA discloses data breach after the recent ransomware attack

The chipmaker company launched an investigation into the incident to determine the extent of the intrusion that confirmed that the attackers have stolen data from the chipmaker.

Cyware News - Latest Cyber News

WordPress-hosted Ukrainian University Websites Hacked in Targeted Attacks

The group, whose members refer to themselves as 'the Mx0nday', have targeted the WordPress-hosted sites more than 100,000 times since February 24, when Russian troops officially invaded Ukraine.

Twitter

bB Rus

RUS/UKR-induced can't sleep mode gave me some time to catch up perusing recent CVEs over at AttackerKB. Almost skipped past CVE-2022-25329 but Novell NetWare caught my eye. That thing has been dead for 5 years. There really are orgs that still use it?

CVE

CVE-2022-25418 Tenda AC9 V15.03.2.21_cn was discovered to contain a stack overflow via the function openSchedWifi.

Debra M. Fezza Reed #SecRiskRptSME #QSC2022

RT: CVE-2022-25329 Trend Micro ServerProtect 6.0/5.8 Information Server uses a static credential to perform authentication when a specific command is typed in the console. An unauthenticated remote attacker with access to the Information Server could ... [...]

()

Security NEXT CVE-2022-25329

CVE-2021-44567 An SQL Injection vulnerability exits in RosarioSIS before 7.6.1 via the votes parameter in

PatrowlHears Alert: CVE-2021-44567 CVSS: 7.5 / CTI Score: 84 / Exploit: 1 An unauthenticated SQL Injection

CVE

ProgramFunctions/PortalPollsNotes.fnc.php.

Threat Intel Center

NEW: CVE-2021-44567 An unauthenticated SQL Injection vulnerability exists in RosarioSIS before 7.6.1 via the votes parameter in ProgramFunctions/PortalPollsNotes.fnc.php. Severity: CRITICAL

Threat Intel Center

NEW: CVE-2021-44567 An unauthenticated SQL Injection vulnerability exists in RosarioSIS before 7.6.1 via the votes parameter in ProgramFunctions/PortalPollsNotes.fnc.php. Severity: CRITICAL

vulnonym

One night, CVE-2021-44567 wished upon a star, and today that wish has been granted. It now has a name, like a real, live vulnerability: Walking Loon

Ron DeSantis

Governor DeSantis is at the University of South Florida to announce investments in cybersecurity workforce education.

PatrOwl

vulnerability exists in RosarioSIS before... #None #Remote #NoAuth More informations: Subscribe online:

Remotely Alerts

Severity: | An unauthenticated SQL Injection vulnera... | CVE-2021-44567 | Link for more:

CVE.report

CVE-2021-44567 : An unauthenticated SQL Injection vulnerability exists in RosarioSIS before 7.6.1 via the votes parameter in ProgramFunctions/PortalPollsNotes.fnc.php....

ThreatMeter

CVE-2021-44567 An unauthenticated SQL Injection vulnerability exists in RosarioSIS before 7.6.1 via the votes parameter in ProgramFunctions/PortalPollsNotes.fnc.php. (CVSS:0.0) (Last Update:2022-02-24)

Source: NIST

NIST CVE: Critical

CVE-2021-44663

A Remote Code Execution (RCE) vulnerability exists in the Xerte Project Xerte through 3.8.4 via a crafted php file through **elfinder** in connetor.php.

	Vector:	Created:	Updated:
CRITICAL	network	2022-02-24	2022-03-03

CVE-2022-25418

Tenda AC9 V15.03.2.21_cn was discovered to contain a stack overflow via the function openSchedWifi.

	Vector:	Created:	Updated:
CRITICAL	network	2022-02-24	2022-03-03

CVE-2021-44567

An unauthenticated SQL Injection vulnerability exists in **RosarioSIS** before 7.6.1 via the votes parameter in ProgramFunctions/PortalPollsNotes.fnc.php.

	Vector:	Created:	Updated:
CRITICAL	network	2022-02-24	2022-03-03

CVE-2022-25329

Trend Micro **ServerProtect** 6.0/5.8 **Information Server** uses a static credential to perform authentication when a specific command is typed in the console. An unauthenticated remote attacker with access to the Information Server could exploit this to register to the server and perform authenticated actions.

	Vector:	Created:	Updated:
CRITICAL	network	2022-02-24	2022-03-03

Source: NIST

NIST CVE: High

CVE-2022-24671

A link following privilege escalation vulnerability in Trend Micro **Antivirus** for Max 11.0.2150 and below could allow a local attacker to modify a file during the update process and escalate their privileges. Please note: an attacker must **first** obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

	Vector:	Created:	Updated:
HIGH	local	2022-02-24	2022-03-03

CVE-2022-0651

The WP **Statistics WordPress** plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the current_page_type parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers without authentication to inject

CVE-2022-24678

An **security agent** resource exhaustion denial-of-service vulnerability in Trend Micro **Apex** One, Trend Micro **Apex One** as a Service, Trend Micro Worry-Free **Business Security** 10.0 SP1 and Trend Micro **Worry-Free Business Security** Services agents could allow an attacker to flood a temporary log location and consume all disk **space** on affected installations.

	Vector:	Created:	Updated:
HIGH	network	2022-02-24	2022-03-03

arbitrary SQL queries to obtain sensitive information, in versions up to and including 13.1.5.

HIGH Vector: network Created: 2022-02-24 Updated: 2022-03-03

Source: NIST

NIST CVE: Medium

CVE-2021-44566

A Cross Site Scripting (XSS) vulnerability exists in **RosarioSIS** before 4.3 via the SanitizeMarkDown function in ProgramFunctions/MarkDownHTML.fnc.php.

MEDIUM Vector: network Created: 2022-02-24 Updated: 2022-03-03

CVE-2021-44565

A Cross Site Scripting (XSS) vulnerability exists in **RosarioSIS** before 7.6.1 via the xss_clean function in classes/Security.php, which allows remote malicious users to inject arbitrary JavaScript or HTML. An example of affected components are all **Markdown** input fields.

MEDIUM Vector: network Created: 2022-02-24 Updated: 2022-03-03

CVE-2021-44662

A Site Scripting (XSS) vulnerability exists in the Xerte Project Xerte through 3.8.4 via the link parameter in **print**.php.

MEDIUM Vector: network Created: 2022-02-24 Updated: 2022-03-03

CVE-2022-24687

HashiCorp Consul and Consul Enterprise 1.8.0 through 1.9.14, 1.10.7, and 1.11.2 has Uncontrolled Resource Consumption.

MEDIUM Vector: network Created: 2022-02-24 Updated: 2022-03-03

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2021-44961

A memory leakage flaw exists in the class PerimeterGenerator of Slic3r libslic3r 1.3.0 and Master Commit b1a5500. Specially crafted stl files can exhaust available memory. An attacker can provide malicious files to trigger this vulnerability.

UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-03

CVE-2022-24573

A stored cross-site scripting (XSS) vulnerability in the admin interface in Element-IT HTTP Commander 7.0.0 allows unauthenticated users to get admin access by injecting a malicious script in the User-Agent field.

UNRATED Vector: unkown Created: 2022-03-03 Updated: 2022-03-03

CVE-2022-25471

An Insecure Direct Object Reference (IDOR) vulnerability in **OpenEMR** 6.0.0 allows any authenticated attacker to access and modify unauthorized areas via a crafted POST request to /modules/zend_modules/public/Installer/register.

UNRATED Vector: unkown Created: 2022-03-03 Updated: 2022-03-03

CVE-2022-24571

Car Driving **School Management System** v1.0 is affected by SQL injection in the login page. An attacker can use simple SQL login injection payload to get admin access.

UNRATED Vector: unkown Created: 2022-02-28 Updated: 2022-03-03

CVE-2021-44343

David Brackeen **ok-file-formats** 203defd is vulnerable to Buffer Overflow. When the function of the ok-file-formats project is used, a heap-buffer-overflow occurred in function ok_png_read_data() in "/ok_png.c".

UNRATED Vector: unkown Created: 2022-03-03 Updated: 2022-03-03

CVE-2021-44335

David Brackeen **ok-file-formats** 203defd is vulnerable to Buffer Overflow. When the function of the ok-file-formats project is used, a heap-buffer-overflow occurs in function ok_png_transform_scanline() in "/ok_png.c:533".

UNRATED Vector: unkown Created: 2022-03-03 Updated: 2022-03-03

CVE-2022-22909

HotelDruid v3.0.3 was discovered to contain a remote code execution

CVE-2022-0528

Exposure of Sensitive Information to an Unauthorized Actor in **GitHub** repository transloadit/uppy prior to 3.3.1.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

CVE-2022-24563

In **Genixcms** v1.1.11, a stored Cross-Site Scripting (XSS) vulnerability exists in /gxadmin/index.php?page=themes&view=options" via the intro_title and intro_image parameters.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

CVE-2021-38269

Liferay Portal through v7.4.0 and Liferay DXP through v7.1 were discovered to contain a cross-site scripting (XSS) vulnerability via the Gogo Shell module.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

CVE-2021-38265

Liferay Portal v7.3.6 and below and Liferay DXP v7.3 and below were discovered to contain a cross-site scripting (XSS) vulnerability via the _com_liferay_asset_list_web_portlet_AssetListPortlet_title parameter.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

CVE-2022-25089

Printix Secure Cloud **Print Management** 1.3.1035.0 incorrectly uses Privileged APIs.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

CVE-2022-23849

The biometric **lock** in **Devolutions** Password Hub for iOS before 2021.3.4 allows attackers to access the application because of authentication bypass. An attacker must rapidly make failed biometric authentication attempts.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

(RCE) vulnerability which is exploited via an attacker inserting a crafted payload into the name field under the Create New Room module.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

CVE-2021-38267

Liferay Portal through v7.3.6 and Liferay DXP through v7.3 were discovered to contain a cross-site scripting (XSS) vulnerability via the Edit **Blog** Entry function under the Blog module.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

CVE-2021-38263

Liferay Portal v7.3.2 and below and Liferay DXP v7.0 and below were discovered to contain a cross-site scripting (XSS) vulnerability via the script console under the Server module.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

CVE-2021-38264

Liferay Portal v7.4.1 and below was discovered to contain a cross-site scripting (XSS) vulnerability via the keywords parameter under the Frontend **Taglib** module.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

CVE-2021-42950

Remote Code Execution (RCE) vulnerability exists in Zepl Notebooks all previous versions before **October** 25 2021. Users can register for an account and are allocated a set number of credits to try the product. Once users authenticate, they can proceed to create a new organization by which additional users can be added for various **collaboration** abilities, which allows malicious user to create new Zepl Notebooks with various languages, contexts, and deployment scenarios. Upon creating a new notebook with specially crafted malicious code, a user can then launch remote code execution.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

CVE-2022-25146

The Remote App module in **Liferay** Portal through v7.4.3.8 and Liferay DXP through v7.4 does not check if the **origin** of event messages it receives matches the origin of the Remote App, allowing attackers to exfiltrate the CSRF token via a crafted event message.

UNRATED | Vector: unkown | Created: 2022-03-03 | Updated: 2022-03-03

Source: Hybrid Analysis

Top malicious files

100% Threat score	payload (.) exe	100% Threat score	CCleaner (.) exe
100% Threat score	Patch (.) exe	100% Threat score	Setup_x32_x64 (.) exe
100% Threat score	Latest invoice with a new address to update (.) xlsm	100% Threat score	ccsetup590_pro_trial (.) exe
100% Threat score	Truecaller v12 (.) 16 (.) 5 [Gold+Orange+Purple+Lite] (.) apk	100% Threat score	tinytag (.) msi
100% Threat score	TrueCaller v12 (.) 15 (.) 6 (.) apk	100% Threat score	RunGame (.) exe
100% Threat score	AnyDesk (.) exe	98% Threat score	15a772d0dcbde0cffde9b58be5007244fd23159daaa67110f53259ffff69b3c9 (.) exe
92% Threat score	exe (.) exe	85% Threat score	gks1 (.) 20 (.) exe
80% Threat score	REvised_Po#240122 (.) html	75% Threat score	Pinner (.) exe
75% Threat score	SABnzbd-3 (.) 5 (.) 1-win-setup (.) exe		

Source: Hybrid Analysis

Top malicious URL

83% Threat score	https://ronemo (.) com/video/mTCgB5o8cL1/VnU3zuegoL	82% Threat score	http://www (.) soscartilagecenterofny (.) com/
81% Threat score	https://ronemo (.) com/video/ZiqaAXsBfm7/VnU3zueasm	81% Threat score	https://ronemo (.) com/video/t30r7NSHZf5/VnU3zuerSf
81% Threat score	https://ronemo (.) com/video/3xL7gpcmerN/76d9kHV7cr	79% Threat score	http://37u5fa3h78 (.) dampierislandtourism (.) com/cmljaGFyZC5mcmFuY2lzQHRpbG5leS5jb20=
77% Threat score	http://mercurypursuitofparadise2021 (.) com/Scripts	72% Threat score	http://xqw7 (.) mjt (.) lu/

Source: SpamHaus

Top spamming countries

	#1 United States of America		#2 China
	#3 Russian Federation		#4 Mexico
	#5 Dominican Republic		#6 Saudi Arabia
	#7 India		#8 Japan
	#9 Brazil		#10 Uruguay

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 United States of America

#4 Thailand

#5 Indonesia

#6 Algeria

#7 Viet Nam

#8 Brazil

#9 Pakistan

#10 Iran (Islamic Republic of)

Source: SpamHaus

Top phishing countries

#1 United States

#2 Germany

#3 Russia

#4 Bulgaria

#5 Hong Kong

#6 Netherlands

#7 Singapore

#8 France

#9 India

#10 Japan

Source: Have I been pwned?

Have I been pwnd

MacGeneration (macg.co)
In January 2022, the French Apple news website MacGeneration suffered a data breach. The incident exposed over 100k usernames, email addresses and passwords stored as salted SHA-512 hashes. After discovering the incident, MacGeneration self-submitted data to HIBP.

Count: 101004 | Created: 2022-01-29 | Updated: 2022-03-03

NVIDIA (nvidia.com)
In February 2022, microchip company NVIDIA suffered a data breach that exposed employee credentials and proprietary code. Impacted data included over 70k employee email addresses and NTLM password hashes, many of which were subsequently cracked and circulated within the hacking community.

Count: 71335 | Created: 2022-02-23 | Updated: 2022-03-02

Source: Imperva DDOS Map

Top DDOS attackers

Source: Imperva DDOS Map

Top DDOS country targets

Source: Imperva DDOS Map

Top DDOS techniques

Source: Imperva DDOS Map

Top DDOS industry targets