Your Security Rabbits report for March 05, 2022

Source: Ransom Watch

Ransomware attacks

alphv	Target: Assimoco Group | assimoco . it(2022-03-05)
ragnarlocker	Target: GHI Hornos Industriales Fully Leaked(2022-03-04)
hiveleak	Target: PAN AMERICAN ENERGY S . L . SUCURSAL ARGENTINA(2022-03-04)
lockbit2	Target: freedomfarmspa . . . . (2022-03-04)
conti	Target: Lifetech Resources(2022-03-04)

Hot topics

Nothing today

News

CyberScoop

Biden administration seeks money to bolster Ukraine war-related cybersecurity at home, abroad

The Biden administration is requesting additional funds from Congress to help Ukraine with its digital defenses, strengthen cybersecurity in Europe and enhance U.S. capabilities to respond to the fallout from the Russian invasion. The overall fiscal 2022 supplemental request, sent to Capitol Hill this week, seeks $10 billion in Ukraine-related needs and $22.5 billion in funding related to COVID-19. Among the bigger pots of cybersecurity-focused funding the administration is requesting is $1.25 billion for the Defense Department to assist Ukraine with support on "operational surges across multiple national defense components, including accelerated cyber capabilities, weapons systems upgrades,[…]

Security Affairs

CISA adds 95 flaws to the Known Exploited Vulnerabilities Catalog

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added 95 vulnerabilities to its Known Exploited Vulnerabilities Catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added 95 vulnerabilities to its Known Exploited Vulnerabilities Catalog. According to Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, FCEB agencies have to address the identified vulnerabilities […] The post CISA adds 95 flaws to the Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.

Cyware News - Latest Cyber

CISA Adds Another 95 Flaws to its Known Exploited Vulnerabilities List

The CISA just added 95 new bugs to its catalog of known exploited vulnerabilities, including multiple critical Cisco router flaws, new and old Windows flaws, bugs in Adobe Flash Player, and more.

The Hacker News

Both Sides in Russia-Ukraine War Heavily Using Telegram for Disinformation and Hacktivism

Cyber criminals and hacktivist groups are increasingly using the Telegram messaging app for their activities, as the Russia-Ukraine conflict enters its eighth day. A new analysis by Israeli cybersecurity company Check Point Research has found that "user volume grew a hundred folds daily on Telegram related groups, peaking at 200,000 per group." Prominent among the groups are anti-Russian cyber

The Hacker News

CISA Adds Another 95 Flaws to its Actively Exploited Vulnerabilities Catalog

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) this week added 95 more security flaws to its Known Exploited Vulnerabilities Catalog, taking the total number of actively exploited vulnerabilities to 478. "These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise," the agency said in an advisory

Blog â€“ Flashpoint

CISA's BOD 22-01 Update: Revamping Vulnerability Management Capabilities for Federal Agencies

The Cybersecurity and Infrastructure Security Agency (CISA) has added 95 more vulnerabilities to Binding Operational Directive (BOD) 22-01, as of March 3. Also known as the Known Exploited Vulnerabilities (KEV) Catalog, BOD 22-01 provides organizations with a curated list of vulnerabilities that have been--or are actively being--exploited in the wild. While only Federal Civilian Executive […] The post CISA's BOD 22-01

News

Krebs on Security

Conti Ransomware Group Diaries, Part III: Weaponry

Part I of this series examined newly-leaked internal chats from the Conti ransomware group, and how the crime gang dealt with its own internal breaches. Part II explored what it's like to be an employee of Conti's sprawling organization. Today's Part III looks at how Conti abused a panoply of popular commercial security services to undermine the security of their targets, as well as how the team's leaders strategized for the upper hand in ransom negotiations with victims.

Cyware News - Latest Cyber News

Elon Musk warns of possible targeted attacks on Starlink in Ukraine

SpaceX chief Elon Musk has expressed his concerns over the future of SpaceX's Starlink service in Ukraine, given the current scenario of uncertainty in the country post the Russian invasion.

CyberScoop

FTC, DOJ settle with WW weight loss app, citing violation of children's privacy

The Federal Trade Commission and Justice Department slapped a children's weight loss app with a $1.5 million penalty and an order to delete data it collected on thousands of children under 13 allegedly without proper parental consent. The complaint from the FTC and DOJ alleges that Kurbo by WW (formerly known as Weight Watchers) failed to properly verify parental consent for users under 13 and made it easy for hundreds of users who identified as 13 or older during the signup process to then later change their age in the app. It also alleges the app didn't properly notify parents who signed up on their children's behalf about the extent of the data collected by the app. Both practices, the FT[...]

Cyware News - Latest Cyber News

Hacktivists, cybercriminals switch to Telegram after Russian invasion

The Telegram messaging app has taken a pivotal role in the ongoing conflict between Russia and Ukraine, as it is being massively used by hacktivists and cybercriminals alike.

Cyware News - Latest Cyber News

How a simple security bug became a university campus 'master key'

For its GET Mobile app, CBORD publishes a list of commands available through its API, which can be controlled using a student's credentials. But the API was not checking if the credentials were valid.

Cyware News - Latest Cyber News

Maryland Officials Outline Package to Tighten Cybersecurity

Maryland lawmakers highlighted a package of measures Wednesday to tighten cybersecurity in the state. One of the measures would increase coordination between state and local governments in cybersecurity.

The Hacker News

New Linux Kernel Cgroups Vulnerability Could Let Attackers Escape Container

Details have emerged about a now-patched high-severity vulnerability in the Linux kernel that could potentially be abused to escape a container in order to execute arbitrary commands on the container host. The shortcoming resides in a Linux kernel feature called control groups, also referred to as cgroups version 1 (v1), which allows processes to be organized into hierarchical groups,

Update: Revamping Vulnerability Management Capabilities for Federal Agencies appeared first on Flashpoint.

Cyware News - Latest Cyber News

Cyberattack on New York State's Joint Commission on Public Ethics Leads to System Outage

The ethics watchdog, which regulates lobbying at the State Capitol, said on Friday that an investigation had been launched to determine the scope of the attack and who was behind it.

Threatpost

Free HermeticRansom Ransomware Decryptor Released

Cruddy cryptography means victims whose files have been encrypted by the Ukraine-tormenting ransomware can break the chains without paying extortionists.

Cyware News - Latest Cyber News

Hackers Leak 190GB of Alleged Samsung Data, Source Code

The Lapsus$ data extortion group leaked today a huge collection of confidential data they claim to be from Samsung Electronics, the South Korean giant consumer electronics company.

Cyware News - Latest Cyber News

Highly Sophisticated FoxBlade Malware Targets Ukrainian Networks

Microsoft laid bare a cyberattack effort involving the FoxBlade malware, which was launched against Ukraine hours before Russia's tanks and missiles began to hit the country. Upon understanding the threat it poses, the firm provided technical advice on how to identify and mitigate the enclosed malicious code. People are requested to watch out for this and not forget to act upon the advisory shared by Microsoft.

The Hacker News

Imperva Thwarts 2.5 Million RPS Ransom DDoS Extortion Attacks

Cybersecurity company Imperva on Friday said it recently mitigated a ransom distributed denial-of-service (DDoS) attack targeting an unnamed website that peaked at 2.5 million requests per second (RPS). "While ransom DDoS attacks are not new, they appear to be evolving and becoming more interesting with time and with each new phase," Nelli Klepfish, security analyst at Imperva, said. "For

Threatpost

Massive Meris Botnet Embeds Ransomware Notes from REvil

Notes threatening to tank targeted companies' stock price were embedded into the DDoS ransomware attacks as a string_of_text directed to CEOs and webops_geeks in the URL.

The Hacker News

New Security Vulnerability Affects Thousands of Self-Managed GitLab Instances

Researchers have disclosed details of a new security vulnerability in GitLab, an open-source DevOps software, that could potentially allow a remote, unauthenticated attacker to recover user-related information. Tracked as CVE-2021-4191 (CVSS score: 5.3), the medium-severity flaw affects all versions of GitLab Community Edition and Enterprise Edition starting from 13.0 and all versions starting

Blog â€“ Flashpoint

Raid Forums Is Down. Who's Behind Its Apparent Seizure?

On February 25, Raid Forums--a popular illicit online community notorious for its high-profile large-scale database leaks--was allegedly seized by an unknown identity. As of this publishing, it is not clear why Raid Forums was taken down, or who was responsible. No official government agency in any country has claimed responsibility for seizing the Raid Forums [...] The post Raid Forums Is Down. Who's Behind Its Apparent Seizure? appeared first on Flashpoint.

Security Affairs

Russian watchdog Roskomnadzor also blocked Facebook in Russia

State communications watchdog Roskomnadzor has ordered to block access to Facebook in Russia amid the ongoing invasion of Ukraine. State communications watchdog Roskomnadzor ordered to block access to Facebook over its decision to ban Russian media and state information resources. The block comes after Facebook recently deactivated or restricted access to accounts belonging to media [...] The post Russian watchdog Roskomnadzor also blocked Facebook in Russia appeared first on Security Affairs.

Cyware News - Latest Cyber News

The New Daxin Network Attack Tool has a Chinese Link

The CISA and Symantec laid bare Daxin, a stealthy backdoor linked to a Chinese hacker group. The highly sophisticated rootkit was used against select governments and other critical infrastructure targets. Organizations are suggested to make use of IOCs that may help in the detection of malicious activity.

Security Affairs

Thousands of satellite users offline in Europe following a cyberattack, is it a conflict spillover?

Thousands of satellite internet users across Europe were disconnected from the internet by a cyber-event, experts suspect a cyber attack. Orange confirmed that "nearly 9,000 subscribers" of a satellite internet service provided by its subsidiary Nordnet in France were offline following a "cyber event" that took place on February 24 at Viasat, the US giant [...] The post Thousands of satellite users offline in Europe following a cyberattack, is it a conflict spillover? appeared first on Security Affairs.

Cyware News - Latest Cyber News

Ukraine to join NATO intel-sharing cyberdefense hub

While Ukraine is yet to become a member of the North Atlantic Treaty Organization (NATO), the country has been accepted as a contributing participant to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

Cyware News - Latest Cyber News

RuRAT Malware Campaign Impersonates Venture Capital Firm Looking to Purchase Sites

BleepingComputer was contacted by an alleged VC firm that wanted to invest or purchase the site. However, it was a malicious campaign designed to install malware providing remote access to devices.

Cyware News - Latest Cyber News

The most impersonated brands in phishing attacks

With six brands in the top 20, financial services was the most impersonated industry of 2021, representing 35% of all phishing pages, rising sharply based on its place at 28% in 2020.

Security Affairs

These are the sources of DDoS attacks against Russia, local NCCC warns

Russian government released a list containing IP addresses and domains behind DDoS attacks that hit Russian infrastructure after the invasion. While the conflict on the battlefield continues, hacktivists continue to target Russian infrastructure exposed online. The Russian National Coordinating Center for Computer Incidents (NCCC) released a massive list containing 17,576 IP addresses and 166 domains that were involved [...] The post These are the sources of DDoS attacks against Russia, local NCCC warns appeared first on Security Affairs.

Cyware News - Latest Cyber News

Ukraine Says Local Government Sites Infiltrated to Push Fake Capitulation News

The SSU said that hackers are using compromised local government and regional authorities' websites to push rumors that Ukraine surrendered and signed a peace treaty with Russia.

CyberScoop

Ukraine, looking to fortify itself against Russian attacks, admitted to NATO cyber center

NATO nations voted unanimously on Friday to admit Ukraine to their Cooperative Cyber Defence Centre of Excellence (CCDCOE), a development which experts said will help Ukraine fight off mounting cyberthreats from Russia. The CCDCOE is a NATO-accredited cyber knowledge hub, research institution and training and exercise facility. "They're one of the leading if not the leading institution for thinking about cyber warfare," said James Lewis, director of the strategic technologies program at the Center for Strategic and International Studies, a Washington think tank. Lewis said the decision to include Ukraine in the CCDCOE will have an immediate impact on its ability to fend off Russian cyberatta[...]

Twitter

Brian

Remember when Trump actually proposed creating an impenetrable Cyber Security unit with Vladimir Putin?

ABC

A top Ukrainian cybersecurity official says a volunteer army of hundreds of hackers enlisted to fight Russia in cyberspace is attacking only what it deems military targets.

Klaas

The Wall Street Journal

Hundreds of thousands of Ukrainian technology workers have taken part in cyberattacks against Russias government, media and financial institutions in recent days, a top Ukrainian cybersecurity official said Friday

Tomi T Ahonen Stands With Ukraine

If you think Russia could not be worse... it could have been. Trump actually suggested THIS - a joint cyberwarfare unit, giving Putin's spies CONTROL of US cyber security. Trump was talked out of it, one of the few times the adults prevailed over America's Toddler-In-Chief

News

FBI

We invite you to tune in to the recorded 2022 Munich Cyber Security Conference, where #FBI Cyber Deputy Assistant Director Tonya Ugoretzalong with other top-level industry and government leadersjoined a discussion on government #cybersecurity priorities.

ChuckGrassley

Clarke Co Farm Bureau 15ppl issues: my cattle market transparency bill + free/reduced lunch + WOTUS + high gas prices + cyber security +inheritance tax + Gov Reynolds state of the union response etc #99countymeetings

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-2021-27757

" Insecure password storage issue.The application stores sensitive information in cleartext within a resource that might be accessible to another control sphere.Since the information is stored in cleartext, attackers could potentially read it and gain access to sensitive information."

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-20303

A flaw found in function dataWindowForTile() of IlmImf/ImfTiledMisc.cpp. An attacker who is able to submit a crafted file to be processed by **OpenEXR** could trigger an integer overflow, leading to an out-of-bounds write on the heap. The greatest impact of this flaw is to application availability, with some potential impact to data integrity as well.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-20302

A flaw was found in OpenEXR's TiledInputFile functionality. This flaw allows an attacker who can submit a crafted single-part non-image to be processed by OpenEXR, to trigger a floating-point exception error. The highest threat from this vulnerability is to system availability.

CVE-2021-27756

"TLS-RSA cipher suites are not disabled in **BigFix** Compliance up to v2.0.5. If TLS 2.0 and secure ciphers are not enabled then an attacker can passively record traffic and later decrypt it."

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-20300

A flaw was found in OpenEXR's hufUncompress functionality in OpenEXR/IlmImf/ImfHuf.cpp. This flaw allows an attacker who can submit a crafted file that is processed by OpenEXR, to trigger an integer overflow. The highest threat from this vulnerability is to system availability.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-3737

A flaw was found in **python**. An improperly handled HTTP response in the HTTP client code of python may allow a remote attacker, who controls the HTTP server, to make the client script enter an infinite loop, consuming CPU time. The highest threat from this vulnerability is to system availability.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-3656

A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD/VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-3575

A heap-based buffer overflow was found in **openjpeg** in **color**.c:379:42 in sycc420_to_rgb when decompressing a crafted .j2k file. An attacker could use this to execute arbitrary code with the permissions of the application compiled against openjpeg.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-20319

An improper signature verification vulnerability was found in coreos-installer. A specially crafted **gzip** installation image can bypass the image signature verification and as a consequence can lead to the installation of unsigned content. An attacker able to modify the original installation image can write arbitrary data, and achieve full access to the node being installed.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-40846

An issue was discovered in Rhinode Trading Paints through 2.0.36. TP **Updater**.exe uses cleartext HTTP to check, and request, updates. Thus, attackers can man-in-the-middle a victim to download a malicious binary in place of the real update, with no SSL errors or **warnings**.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-26484

An issue was discovered in **Veritas InfoScale Operations Manager** (VIOM) before 7.4.2 Patch 600 and 8.x before 8.0.0 Patch 100. The web server fails to sanitize admin/cgi-bin/rulemgr.pl/getfile/ input data, allowing a remote authenticated administrator to read arbitrary files on the system via Directory Traversal. By manipulating the resource name in GET requests referring to files with absolute paths, it is possible to access arbitrary files stored on the filesystem, including application source code, configuration files, and critical system files.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-25106

D-Link DIR-859 v1.05 was discovered to contain a stack-based buffer overflow via the function genacgi_main. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-3428

A flaw was found in the **Linux** kernel. A denial of service problem is identified if an extent tree is corrupted in a crafted ext4 filesystem in fs/ext4/extents.c in ext4_es_cache_extent. Fabricating an integer overflow, A local attacker with a special user privilege may cause a system crash problem which can lead to an availability threat.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-21828

A user with high privilege access to the Incapptic **Connect web console** can remotely execute code on the Incapptic Connect server using a unspecified attack vector in Incapptic Connect version 1.40.0, 1.39.1, 1.39.0, 1.38.1, 1.38.0, 1.37.1, 1.37.0, 1.36.0, 1.35.5, 1.35.4 and 1.35.3.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-46353

An information disclosure in **web interface** in **D-Link** DIR-X1860 before 1.03 RevA1 allows a remote unauthenticated attacker to send a specially crafted HTTP request and gain knowledge of different absolute paths that are being used by the web application.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-26483

An issue was discovered in **Veritas InfoScale Operations Manager** (VIOM) before 7.4.2 Patch 600 and 8.x before 8.0.0 Patch 100. A reflected cross-site scripting (XSS) vulnerability in admin/cgi-bin/listdir.pl allows authenticated remote administrators to inject arbitrary web script or HTML into an HTTP GET parameter (which reflect the user input without sanitization).

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-25312

An XML external entity (XXE) injection vulnerability was discovered in the Any23 RDFa XSLTStylesheet extractor and is known to affect Any23 versions < 2.7. XML external entity injection (also known as XXE) is a **web security** vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the **application server** filesystem, and to **interact** with any back-end or external systems that the application itself can access. This issue is fixed in **Apache** Any23 2.7.

UNRATED Vector: unkown Created: 2022-03-05 Updated: 2022-03-05

CVE-2021-43590

Dell EMC **Enterprise Storage** Analytics for vRealize Operations, versions 4.0.1 to 6.2.1, contain a Plain-text password storage vulnerability. A local high privileged malicious user may potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.

CVE-2022-25465

Espruino 2v11 release was discovered to contain a stack buffer overflow via src/jsvar.c in jsvGetNextSibling.

UNRATED Vector: unkown Created: 2022-03-05 Updated: 2022-03-05

CVE-2021-46384

https://gitee.com/mingSoft/MCMS MCMS <=5.2.5 is affected by: RCE. The impact is: execute arbitrary code (remote). The attack vector is: ${"freemarker.template.utility.Execute"?new()("calc")}. PP MCMS has a pre-auth RCE vulnerability through which allows unauthenticated attacker with network access via http to compromise MCMS. Successful attacks of this vulnerability can result in takeover of MCMS.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-25069

Mark Text v0.16.3 was discovered to contain a DOM-based cross-site scripting (XSS) vulnerability which allows attackers to perform remote code execution (RCE) via injecting a crafted payload into /lib/contentState/pasteCtrl.js.

UNRATED Vector: unkown Created: 2022-03-05 Updated: 2022-03-05

CVE-2022-23232

StorageGRID (formerly StorageGRID Webscale) versions prior to 11.6.0 are susceptible to a vulnerability which when successfully exploited could allow disabled, expired, or locked external user accounts to access S3 data to which they previously had access. StorageGRID 11.6.0 obtains the user account **status** from Active Directory or **Azure** and will block S3 access for disabled user accounts during the subsequent background synchronization. User accounts that are expired or locked for Active Directory or Azure, or user accounts that are disabled, expired, or locked in identity sources other than Active Directory or Azure must be manually removed from group memberships or have their S3 keys manually removed from Tenant Manager in all versions of StorageGRID (formerly StorageGRID Webscale).

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-23915

The package **weblate** from 0 and before 4.11.1 are vulnerable to Remote Code Execution (RCE) via argument injection when using git or **mercurial** repositories. Authenticated users, can change the behavior of the application in an unintended way, leading to command execution.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-44827

There is remote authenticated OS command injection on **TP-Link Archer** C20i 0.9.1 3.2 v003a.0 Build 170221 Rel.55462n devices vie the X_TP_ExternalIPv6Address HTTP parameter, allowing a remote attacker to run arbitrary commands on the router with root privileges.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-0849

Use After Free in r_reg_get_name_idx in **GitHub**

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-25044

Espruino 2v11.251 was discovered to contain a stack buffer overflow via src/jsvar.c in jsvNewFromString.

UNRATED Vector: unkown Created: 2022-03-05 Updated: 2022-03-05

CVE-2022-0855

Improper Resolution of Path Equivalence in **GitHub** repository microweber-dev/whmcs_plugin prior to 0.0.4.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-26318

On **WatchGuard** Firebox and XTM appliances, an unauthenticated user can execute arbitrary code, aka FBX-22786. This vulnerability impacts **Fireware** OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-23233

StorageGRID (formerly StorageGRID Webscale) versions prior to 11.6.0 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS) of the Local Distribution Router (LDR) service.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-25623

The **Symantec** Management Agent is susceptible to a privilege escalation vulnerability. A low privilege local account can be elevated to the SYSTEM level through **registry** manipulations.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2021-32008

This issue affects: **Secomea** GateManager Version 9.6.621421014 and all prior versions. Improper Limitation of a Pathname to restricted directory, allows logged in GateManager admin to delete system Files or Directories.

UNRATED Vector: unkown Created: 2022-03-04 Updated: 2022-03-05

CVE-2022-24727

Weblate is a web based localization tool with tight version control integration. Prior to version 4.11.1, Weblate didn't properly sanitize some arguments passed to Git and Mercurial, allowing repository radareorg/radare2 prior to 5.6.6.

UNRATED	Vector: unkown	Created: 2022-03-05	Updated: 2022-03-05

them to change their behavior in an unintended way. Instances where untrusted users cannot create new components are not affected. The issues were fixed in the 4.11.1 release.

UNRATED	Vector: unkown	Created: 2022-03-04	Updated: 2022-03-05

Source: Hybrid Analysis

Top malicious files

100% Threat score	PL9S2eyKezxG (.) dll
100% Threat score	06bcc0c3da4a9734ca0339582cc83cf3
100% Threat score	6f93ac0b9408e18cfeec7b33671ffae6
100% Threat score	Patch (.) exe
100% Threat score	rat (.) exe
100% Threat score	Patch (.) exe
100% Threat score	df5e94a649025801aa2e9c4e0bc8197de1ea12fde5ecab80042891fe68109a31 (.) bin (.) exe
88% Threat score	96fadf93be0e7810ac435d1d53bc10ca
83% Threat score	6c6eaebc8e8008cf0c1c27c1f5e792cb
83% Threat score	9abc897db0dc6e6c33948d753a68369a
83% Threat score	c1a09313214df5773c26700bd44d389d
83% Threat score	2b0c53c56af7819031889974a6fa25cf
78% Threat score	c4e420339f1bed5113d47569c8d51778
75% Threat score	SPSSStatistics (.) exe
71% Threat score	44b4d1ed55e7dc0fb4280bc63b7bfa71

100% Threat score	3596752 (.) pdf
100% Threat score	e852ff6917cee1bf934d207cdc14974c
100% Threat score	bffbce809697baa7c862a5c9360e3bb0
100% Threat score	Nero 2020 - Crack+Patch+Serial (.) exe
100% Threat score	Spotify Checker By DJR - Cracked by FullMoonSword (.) exe
100% Threat score	Form (.) xlsm
100% Threat score	Insidious (.) exe
85% Threat score	Setup (.) exe
83% Threat score	b65d55ec8c3405c3850432310f06571a
83% Threat score	e86284bac056cd840fa90672aa5c1090
83% Threat score	76313995d1955935186ac5dd0e9667aa
80% Threat score	RecoverKeysInstaller (.) exe
77% Threat score	sup (.) dll
72% Threat score	71b5a3830c27dc402a4503fd66a84a71

Source: Hybrid Analysis

Top malicious URL

94% Threat score	http://swayequation (.) top/Ldyinddew/tb (.) php?zyfnwzgz1646463760120
81% Threat score	https://ronemo (.) com/video/LD0lmwQg8A5/u7AvMURlQA

82% Threat score	http://ushaarmour (.) com/
81% Threat score	https://ronemo (.) com/video/JEyq_s4efQR/2N8FrmPq4Q

77%
Threat score

http://bhihv (.) smtpgaze (.) com/tracking/qaR9ZGLkZQx1BQt2ZmL4AGpmZQZjAPM5qzS4qaR9ZQbjJN

76%
Threat score

https://ronemo (.) com/video/Bbafe3zVjEA/u7AvMURfzE

76%
Threat score

https://ronemo (.) com/video/RjkyGfePCdD/2N8FrmPyed

72%
Threat score

http://www (.) loveheadphone (.) co (.) uk/This

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 Netherlands
- #3 Russia
- #4 Germany
- #5 Hong Kong
- #6 Japan
- #7 France
- #8 Singapore
- #9 Canada
- #10 Belgium

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

- **Germany (28%)**
- **United States (18%)**
- **Singapore (9%)**

Source: Imperva DDOS Map

Top DDOS country targets

- **Russia (78%)**
- **Ukraine (14%)**
- **United States (3%)**

Source: Imperva DDOS Map

Top DDOS techniques

92%	**DDoS**
5%	**Automated Threat**
3%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

80%	**Financial Services**
15%	**Business**
1%	**Healthcare**