



Your Security Rabbits report for April 12, 2022

Source: [Ransom Watch](#)











Ransomware attacks

alphv	Florida International University (www.fiu.edu)	quantum	Service Employees' International Union
stormous	Success Neeti	alphv	North Carolina A&T State University (www.ncat.edu)
cuba	tavistock	stormous	National Rehabilitation Training Center
alphv	tgs.com.ar	quantum	JetStar
quantum	Hi Tech HoneyComb	stormous	Epic Games Data Breach
stormous	Delhi Heights School	alphv	DC ADVISORY
alphv	wallyedgar.com Wally Edgar Chevrolet	alphv	bet9ja.com goldbet.it
stormous	ALAM LMS	clop	ZISSERFAMILYLAW.COM
quantum	Wolfe Industrial	lorenz	Advizrs
clop	SLIMSTOCK.COM	clop	SA1SOLUTIONS.COM
conti	Newlat Food SPA	lockbit2	lee-associate
conti	CAE Services	quantum	Broadleaf
lockbit2	azcomputerlabs....		

Hot topics

Nothing today

News

 CYWARE SOCIAL Cyware News - Latest Cyber News	Access control vulnerability in Easy!Appointments platform exposed sensitive personal data An access control vulnerability in open-source scheduling platform Easy!Appointments gave unauthenticated attackers easy access to personally identifiable information (PII), a security researcher has revealed.	 Security Affairs	Anonymous hacked Russia's Ministry of Culture and leaked 446 GB The Anonymous collective has hacked Russia's Ministry of Culture and leaked 446 GB of data through the DDoSecrets platform. Data leak service DDoSecrets has published over 700 GB of data allegedly stolen from the Russian government, including over 500,000 emails. The dump includes three datasets, the largest one is related to the Ministry of Culture [...] The post Anonymous hacked Russia's Ministry of Culture and leaked 446 GB appeared first on Security Affairs.
 CYWARE SOCIAL Cyware News - Latest Cyber News	Artificial intelligence and cybersecurity among top priorities for Brazilian banks Artificial intelligence (AI) and cybersecurity are among the top priorities when it comes to the technology strategy of banking institutions in Brazil, a new study has found.	 CYWARE SOCIAL Cyware News - Latest Cyber News	AWS RDS Vulnerability Leads to AWS Internal Service Credentials Lightspin's Research Team obtained credentials to an internal AWS service by exploiting a local file read vulnerability on the RDS EC2 instance using the log_fdw extension.
 Security Affairs	CISA adds WatchGuard flaw to its Known Exploited Vulnerabilities Catalog The U.S. CISA added the CVE-2022-23176 flaw in WatchGuard Firebox and XTM appliances to its Known Exploited Vulnerabilities Catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the CVE-2022-23176 flaw in WatchGuard Firebox and XTM appliances to its Known Exploited Vulnerabilities Catalog. According to Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, [...] The post CISA adds WatchGuard flaw to its Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.	 IT Security Guru	CISA warns of Russian state hackers exploiting WatchGuard bug The Cybersecurity and Infrastructure Security Agency has warned of Russian state actors exploiting a bug impacting WatchGuard Firebox and XTM firewall appliances. Sandworm, a Russian-sponsored hacking group, believed to be part of the GRU Russian military intelligence agency, reportedly exploited the high severity privilege escalation flaw (CVE-2022-23176) to develop a new botnet, dubbed "Cyclops Blink", [...] The post CISA warns of Russian state hackers exploiting WatchGuard bug appeared first on IT Security Guru.
 CYWARE SOCIAL Cyware News - Latest Cyber News	CISA warns orgs of WatchGuard bug exploited by Russian state hackers The flaw can only be exploited if they are configured to allow unrestricted management access from the Internet. By default, all WatchGuard appliances are configured for restricted management access.	 Krebs on Security	Double-Your-Crypto Scams Share Crypto Scam Host Online scams that try to separate the unwary from their cryptocurrency are a dime a dozen, but a great many seemingly disparate crypto scam websites tend to rely on the same dodgy infrastructure providers to remain online in the face of massive fraud and abuse complaints from their erstwhile customers. Here's a closer look at hundreds of phony crypto investment schemes that are all connected through a hosting provider which caters to people running crypto scams.
 cyberscoop CyberScoop	Federal prosecutors going after alleged Russian hacker mistakenly turn over unrelated case documents, lawyer says The material includes information on non-related people and phone records, and Russian businessmen possibly associated with the Trump administration, according to a court document. The post Federal prosecutors going after alleged Russian hacker mistakenly turn over unrelated case documents, lawyer	 Security Affairs	FFDroider, a new information-stealing malware disguised as Telegram app Cybersecurity researchers spotted a new Windows information-stealing malware, named FFDroider, designed to steal credentials and cookies. Cybersecurity researchers from Zscaler ThreatLabz warn of a new information-stealing malware, named FFDroider, that disguises itself as the popular instant messaging app Telegram. The malware was derived to siphon credentials and cookies from infected machines. "Recently, ThreatLabz identified a novel

says appeared first on CyberScoop.

cyberscoop

CyberScoop

Google files suit against Cameroonian cybercriminal who used puppies as lures
The scams are just the latest example in booming cybercrime using cute puppies to steal money. The post Google files suit against Cameroonian cybercriminal who used puppies as lures appeared first on CyberScoop.

CYWARE SOCIAL

Cyware News - Latest Cyber News

HelpSystems acquires Terranova Security to offer security awareness solutions for businesses
HelpSystems announced the acquisition of Terranova Security, an organization providing phishing simulation, privacy awareness, and security awareness training services across the globe.

threatpost

Threatpost

Microsoft Takes Down Domains Used in Cyberattack Against Ukraine
The APT28 (Advanced persistence threat) is operating since 2009, this group has worked under different names such as Sofacy, Sednit, Strontium Storm, Fancy Bear, Iron Twilight, and Pawn.

The Hacker News

The Hacker News

NGINX Shares Mitigations for Zero-Day Bug Affecting LDAP Implementation
The maintainers of the NGINX web server project have issued mitigations to address security weaknesses in its Lightweight Directory Access Protocol (LDAP) Reference Implementation. "NGINX Open Source and NGINX Plus are not themselves affected, and no corrective action is necessary if you do not use the reference implementation," Liam Crilly and Timo Stark of F5 Networks said in an advisory

CYWARE SOCIAL

Cyware News - Latest Cyber News

Operation Bearded Barbie Aims to Catfish Israeli Officials
AridViper APT group was found targeting high-ranking Israeli officials in a cyberespionage campaign to spy and steal data by compromising their systems and mobile devices. The attackers have created various fake Facebook profiles with fabricated identities and stolen or AI-generated images of good-looking women.

The Hacker News

The Hacker News

Over 16,500 Sites Hacked to Distribute Malware via Web Redirect Service
A new traffic direction system (TDS) called Parrot has been spotted leveraging tens of thousands of compromised websites to launch further malicious campaigns. "The TDS has infected various web servers hosting more than 16,500 websites, ranging from adult content sites, personal websites, university sites, and local government sites," Avast researchers Pavel Novak and Jan Rubin said in a report

CYWARE SOCIAL

Cyware News - Latest Cyber News

Patient data stolen ahead of East Tennessee Children's Hospital attack, outage
Several weeks after a cyberattack spurred network disruptions at ETCH, it is notifying an undisclosed number of patients and parents that the threat actors stole sensitive health information during the incident.

The Hacker News

The Hacker News

Researchers warn of FFDroider and Lightning info-stealers targeting users in the wild
Cybersecurity researchers are warning of two different information-stealing malware, named FFDroider and Lightning Stealer, that are capable of siphoning data and launching further attacks. "Designed to send stolen credentials and cookies to a Command & Control server, FFDroider disguises itself on victim's machines to look like the instant messaging application 'Telegram,'" Zscaler ThreatLabz

CYWARE SOCIAL

Cyware News - Latest Cyber News

Senior EU officials were targeted with Israeli spyware
European Justice Commissioner Didier Reynders and at least four commission staffers were targeted, according to a Reuters report, citing two EU officials and documentation.

CYWARE SOCIAL

Cyware News - Latest Cyber News

Think Like a Criminal: Knowing Popular Attack Techniques to Stop Bad Actors Faster
Analyzing the attack goals of adversaries is important to be able to better align defenses against the speed of changing attack techniques and effectively shut down malware's methods for getting in and making itself at home.

CYWARE SOCIAL

Cyware News - Latest Cyber News

UK: Fraudster Steal over \$75m in 2021 Via Remote Access Tools
Some 20,144 individuals fell victim to such "remote access tool" (RAT) scams in 2021, according to Action Fraud, the UK's national reporting centre for fraud and cybercrime.

FLASHPOINT

Blog â€” Flashpoint

Why the Full Vulnerability Intelligence Picture Depends on Data Beyond CVE/NVD
If your risk models are missing nearly one-third of all known vulnerabilities, are they effective? The Common Vulnerabilities and Exposures (CVE) database has become the unofficial "official" source for disclosed vulnerabilities. Nearly every organization's vulnerability management framework relies on it in one form or another, and whenever vulnerabilities are communicated, CVE IDs are often the

windows [...] The post FFDroider, a new information-stealing malware disguised as Telegram app appeared first on Security Affairs.

The Hacker News

The Hacker News

Google Sues Scammer for Running 'Puppy Fraud Scheme' Website
Google on Monday disclosed that it's taking legal action against a nefarious actor who has been spotted operating fraudulent websites to defraud unsuspecting people into buying non-existent puppies. "The actor used a network of fraudulent websites that claimed to sell basset hound puppies -- with alluring photos and fake customer testimonials -- in order to take advantage of people during the

CYWARE SOCIAL

Cyware News - Latest Cyber News

Lawmakers ask Energy Department to take point on sector digital security
A bipartisan group of House and Senate lawmakers late last week urged the head of the U.S. Energy Department to take the lead in shaping the massive energy sector's cybersecurity.

Security Affairs

Security Affairs

Microsoft's Autopatch feature improves the patch management process
Microsoft announced a feature called Autopatch that will allow organizations to keep their systems up-to-date starting with Windows Enterprise E3 (July 2022). Microsoft recently announced the implementation of a new feature called Autopatch starting with Windows Enterprise E3 in July 2022 that aims at keeping their systems up-to-date. The move aims at improving the patch management process in enterprises [...] The post Microsoft's Autopatch feature improves the patch management process appeared first on Security Affairs.

SOPHOS

Naked Security

OpenSSH goes Post-Quantum, switches to qubit-busting crypto by default
Useful quantum computers might not actually be possible. But what if they are? And what if they arrive, say, tomorrow?

CYWARE SOCIAL

Cyware News - Latest Cyber News

Organizations must be doing something good: Payment fraud activity is declining
Results from an Association for Financial Professionals (AFP) survey are encouraging, as 71% of organizations report having been victims of payments fraud activity in 2021, lower than the 81% reported in 2019.

CYWARE SOCIAL

Cyware News - Latest Cyber News

Parrot TDS: A New Web Redirect Service
Avast laid bare an attack campaign abusing the new Parrot TDS, which has infected over 16,500 websites across different verticals, to deliver RATs via bogus browser update prompts. The campaign started in February, while the signs of Parrot activity have been traced back to October last year. Experts recommend using up-to-date internet security solutions while browsing the web for better protection.

IT Security GURU

IT Security Guru

Pegasus spyware targeted EU officials
Several senior European Union (EU) officials were reportedly targeted with Pegasus spyware last year. Among those targeted were European Justice Commissioner Didier Reynders and at least four other commission staff. Reuters has said that it was notified of the claims by two EU officials and documentation it had reviewed. The EU commission reportedly became aware [...] The post Pegasus spyware targeted EU officials appeared first on IT Security Guru.

CYWARE SOCIAL

Cyware News - Latest Cyber News

Russia-linked Cyclops Blink Botnet Taken Down
The FBI announced taking down the Cyclops Blink botnet, which used to target firewall appliances and SOHO networking devices. It was under the control of the Russian Sandworm group. The operation's initial court authorization was given on March 18, the botnet infection was fully removed from all identified Watchguard devices. The FBI suggested adopting Watchguard's detection and remediation steps for remediating any infection by the malware.

Security Affairs

Security Affairs

SuperCare Health discloses a data breach that Impacted +300K people
SuperCare Health, a leading respiratory care provider in the Western U.S, disclosed a data breach that impacted more than 300,000 individuals. SuperCare Health disclosed a security breach that has led to the exposure of personal information belonging to its patients, patients/members of its partner organizations and others. The company notified impacted individuals and law enforcement [...] The post SuperCare Health discloses a data breach that Impacted +300K people appeared first on Security Affairs.

CYWARE SOCIAL

Cyware News - Latest Cyber News

Third npm protestware: 'event-source-polyfill' calls Russia out
Most recently, the developer of the 'event-source-polyfill' npm package has peacefully protested Russia's "unreasonable invasion" of Ukraine, to Russian consumers by showing anti-war messages in version 1.0.26.

IT Security GURU

IT Security Guru

What Real-Life SaaS Attack Misconfiguration Exploits Can Teach Us
It's unfortunate, but true: SaaS attacks continue to increase. You can't get around it, COVID-19 accelerated the already exploding SaaS market and caused industries not planning on making a switch to embrace SaaS. With SaaS apps becoming the default system of record for organizations, it has left many struggling to secure their company's SaaS estate. [...] The post What Real-Life SaaS Attack Misconfiguration Exploits Can Teach Us appeared first on IT Security Guru.

ZDNet

ZDNet | security RSS

XSS vulnerability patched in Directus data engine platform
The platform is described as a "flexible powerhouse for engineers."

[...] The post Why the Full Vulnerability Intelligence Picture Depends on Data Beyond CVE/NVD appeared first on Flashpoint.

Twitter



huntr
Hacktivity

Server-Side Request Forgery (SSRF) in (CVE-2022-0990) reported by michaellrowley - Patch: #bugbounty #infosec #opensource



Threat
Intel
Center

NEW: CVE-2022-1165 The Blackhole for Bad Bots WordPress plugin before 3.3.2 uses headers such as CF-CONNECTING-IP, CLIENT-IP etc to determine the IP address of requests hitting the blackhole URL, which allows ... (click for more)



Threat
Intel
Center

NEW: CVE-2022-26585 Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list.



Robo
Shadow
Alerts

Potentially Critical CVE Detected! CVE-2022-26585 Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list.... CVSS: 9.33 #Mingsoft #CVE #CyberSecurity



vulnonym

CVE-2022-26585 is called Equable Inanga



Hernan
Espinoza

CVEnew: CVE-2022-26585 Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list.



Bitcoin
News

The event sought to equip officials from countries in this region with more insights on issues that relate to #financial inclusion and cybersecurity. #cbdc #financialinclusion



Vulmon
Vulnerability
Feed

CVE-2022-0990 Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.18.



CVE.report

CVE-2022-26585 : Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list....



CVE

CVE-2022-26585 Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list.



Threat
Intel
Center

NEW: CVE-2022-26585 Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list.



Vulmon
Vulnerability
Feed

CVE-2022-26585 Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list. Don't wait vulnerability scanning results:



eyetsystems

CVE-2022-26585 Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list.

Source: *NIST*

NIST CVE: Critical

CVE-2022-26585

Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list.

CRITICAL Vector: **network** Created: 2022-04-05 Updated: 2022-04-12

CVE-2022-1165

The Blackhole for Bad Bots **WordPress** plugin before 3.3.2 uses headers such as CF-CONNECTING-IP, CLIENT-IP etc to **determine** the IP address of requests hitting the blackhole URL, which allows them to be spoofed. This could result in blocking arbitrary IP addresses, such as legitimate/good search engine crawlers / bots. This could also be abused by competitors to cause damage related to visibility in search engines, can be used to bypass arbitrary blocks caused by this plugin, block any visitor or even the administrator and even more.

CRITICAL Vector: **network** Created: 2022-04-04 Updated: 2022-04-12

CVE-2022-0990

Server-Side Request Forgery (SSRF) in **GitHub** repository janeczku/calibre-web prior to 0.6.18.

CRITICAL Vector: **network** Created: 2022-04-04 Updated: 2022-04-12

Source: *NIST*

NIST CVE: High

CVE-2021-43464

A Remote Code Execution (RCE) vulnerability exists in **Subrion** CMS 4.2.1 via modified code in a background field; when the information is modified, the data in it will be executed through eval().

HIGH Vector: **network** Created: 2022-04-04 Updated: 2022-04-12

CVE-2020-28062

An Access Control vulnerability exists in **HisiPHP** 2.0.11 via special packets that are constructed in \$files = Dir::getList(\$decompath. '/' Upload/Plugins /, which could let a remote malicious user execute arbitrary code.

HIGH Vector: **network** Created: 2022-04-04 Updated: 2022-04-12

CVE-2022-26619

Halo Blog CMS v1.4.17 was discovered to allow attackers to upload arbitrary files via the Attachment Upload function.

HIGH Vector: **network** Created: 2022-04-05 Updated: 2022-04-12

CVE-2022-24785

Moment.js is a JavaScript **date** library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.

HIGH Vector: **network** Created: 2022-04-04 Updated: 2022-04-12

CVE-2022-0809

Out of bounds memory access in WebXR in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

HIGH Vector: **network** Created: 2022-04-05 Updated: 2022-04-12

CVE-2022-27442

TPCMS v3.2 allows attackers to access the **ThinkPHP** log directory and obtain sensitive information such as the administrator's user name and password.

HIGH Vector: **network** Created: 2022-04-04 Updated: 2022-04-12

CVE-2022-0808

Use after free in **Chrome** OS Shell in **Google Chrome** on **Chrome OS** prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in a series of user interaction to potentially exploit heap corruption via user interactions.

CVE-2022-26572

Xerox ColorQube 8580 was discovered to contain an access control issue which allows attackers to print, view the status, and obtain sensitive information.

Source: [NIST](#)

NIST CVE: Medium

CVE-2022-24814	<p>Directus is a real-time API and App dashboard for managing SQL database content. Prior to version 9.7.0, unauthorized JavaScript (JS) can be executed by inserting an iframe into the rich text html interface that links to a file uploaded HTML file that loads another uploaded JS file in its script tag. This satisfies the regular content security policy header, which in turn allows the file to run any arbitrary JS. This issue was resolved in version 9.7.0. As a workaround, disable the live embed in the what-you-see-is-what-you-get by adding <code>`{ "media live embeds": false }`</code> to the <code>_Options Overrides_</code> option of the Rich Text HTML interface.</p> <div>MEDIUMVector: networkCreated: 2022-04-04Updated: 2022-04-12</div>	CVE-2022-1166	<p>The JobMonster Theme was vulnerable to Directory Listing in the <code>/wp-content/uploads/jobmonster/</code> folder, as it did not include a default PHP file, or <code>.htaccess</code> file. This could expose personal data such as people's resumes. Although Directory Listing can be prevented by securely configuring the web server, vendors can also take measures to make it less likely to happen.</p> <div>MEDIUMVector: networkCreated: 2022-04-04Updated: 2022-04-12</div>
----------------	---	---------------	---

Source: [NIST](#)

NIST CVE: Low

Nothing today

Source: [NIST](#)

NIST CVE: Unrated

CVE-2022-1262	<p>A command injection vulnerability in the protest binary allows an attacker with access to the remote command line interface to execute arbitrary commands as root.</p> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-25796	<p>A Double Free vulnerability allows remote malicious actors to execute arbitrary code on DWF file in Autodesk Navisworks 2022 within affected installations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.</p> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-0552	<p>A flaw was found in the original fix for the netty-codec-http CVE-2021-21409, where the OpenShift Logging <code>openshift-logging/elasticsearch6-rhel8</code> container was incomplete. The vulnerable netty-codec-http maven package was not removed from the image content. This flaw affects origin-aggregated-logging versions 3.11.</p> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-25790	<p>A maliciously crafted DWF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 and Autodesk Navisworks 2022 can be used to write beyond the allocated boundaries when parsing the DWF files. Exploitation of this vulnerability may lead to code execution.</p> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-25789	<p>A maliciously crafted DWF, 3DS and DWFX files in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to trigger use-after-free vulnerability. Exploitation of this vulnerability may lead to code execution.</p> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-27528	<p>A maliciously crafted DWFX and SKP files in Autodesk Navisworks 2022 can be used to trigger use-after-free vulnerability. Exploitation of this vulnerability may lead to code execution.</p> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-25792	<p>A maliciously crafted DXF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 and Autodesk Navisworks 2022 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability can be exploited to execute arbitrary code.</p> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-25791	<p>A Memory Corruption vulnerability for DWF and DWFX files in Autodesk AutoCAD 2022, 2021, 2020, 2019 and Autodesk Navisworks 2022 may lead to code execution through maliciously crafted DLL files.</p> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-22572	<p>A non-admin user with user management permission can escalate his privilege to admin user via password reset functionality. The vulnerability affects Incapptic Connect version < 1.40.1.</p> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-22254	<p>A permission bypass vulnerability exists when the NFC CAs access the TEE.Successful exploitation of this vulnerability may affect data confidentiality.</p> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-28347	<p>A SQL injection issue was discovered in <code>QuerySet.explain()</code> in Django 2.2 before 2.2.28, 3.2 before 3.2.13, and 4.0 before 4.0.4. This occurs by passing a crafted dictionary (with dictionary expansion) as the <code>**options</code> argument, and placing the injection payload in an option name.</p> <div>UNRATEDVector: unknownCreated: 2022-04-12Updated: 2022-04-12</div>	CVE-2022-25650	<p>A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.27), Mendix Applications using Mendix 8 (All versions < V8.18.14), Mendix Applications using Mendix 9 (All versions < V9.12.0), Mendix Applications using Mendix 9 (V9.6) (All versions < V9.6.3). When querying the database, it is possible to sort the results using a protected field. With this an authenticated attacker could extract information about the contents of a protected field.</p> <div>UNRATEDVector: unknownCreated: 2022-04-12Updated: 2022-04-12</div>
CVE-2022-27241	<p>A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions), Mendix Applications using Mendix 8 (All versions), Mendix Applications using Mendix 9 (All versions < V9.11). Applications built with an affected system publicly expose the internal project structure. This could allow an unauthenticated remote attacker to read confidential information.</p> <div>UNRATEDVector: unknownCreated: 2022-04-12Updated: 2022-04-12</div>	CVE-2022-28328	<p>A vulnerability has been identified in SCALANCE W1788-1 M12 (All versions < V3.0.0), SCALANCE W1788-2 EEC M12 (All versions < V3.0.0), SCALANCE W1788-2 M12 (All versions < V3.0.0), SCALANCE W1788-2IA M12 (All versions < V3.0.0). Affected devices do not properly handle malformed Multicast LLC frames. This could allow an attacker to trigger a denial of service condition.</p> <div>UNRATEDVector: unknownCreated: 2022-04-12Updated: 2022-04-12</div>
CVE-2022-28329	<p>A vulnerability has been identified in SCALANCE W1788-1 M12 (All versions < V3.0.0), SCALANCE W1788-2 EEC M12 (All versions < V3.0.0), SCALANCE W1788-2 M12 (All versions < V3.0.0), SCALANCE W1788-2IA M12 (All versions < V3.0.0). Affected devices do not properly handle malformed TCP packets received over the RemoteCapture feature. This could allow an attacker to lead to a denial of service condition which only affects the port used by the RemoteCapture feature.</p> <div>UNRATEDVector: unknownCreated: 2022-04-12Updated: 2022-04-12</div>	CVE-2022-27481	<p>A vulnerability has been identified in SCALANCE W1788-1 M12 (All versions < V3.0.0), SCALANCE W1788-2 EEC M12 (All versions < V3.0.0), SCALANCE W1788-2 M12 (All versions < V3.0.0), SCALANCE W1788-2IA M12 (All versions < V3.0.0). Affected devices do not properly handle resources of ARP requests. This could allow an attacker to cause a race condition that leads to a crash of the entire device.</p> <div>UNRATEDVector: unknownCreated: 2022-04-12Updated: 2022-04-12</div>
CVE-2022-25751	<p>A vulnerability has been identified in SCALANCE X302-7 EEC (230V), SCALANCE X302-7 EEC (230V, coated), SCALANCE X302-7 EEC (24V), SCALANCE X302-7 EEC (24V, coated), SCALANCE X302-7 EEC (2x 230V), SCALANCE X302-7 EEC (2x 230V, coated), SCALANCE X302-7</p>	CVE-2022-25752	<p>A vulnerability has been identified in SCALANCE X302-7 EEC (230V), SCALANCE X302-7 EEC (230V, coated), SCALANCE X302-7 EEC (24V), SCALANCE X302-7 EEC (24V, coated), SCALANCE X302-7 EEC (2x 230V), SCALANCE X302-7 EEC (2x 230V, coated), SCALANCE X302-7 EEC (2x 24V), SCALANCE X302-7 EEC (2x 24V, coated), SCALANCE</p>

	<p>on front), SIPLUS NET SCALANCE X308-2. Affected devices do not properly validate if a certain SNMP key exists. An attacker could use this to trigger a reboot of an affected device by requesting specific SNMP information from the device.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-25622	<p>A vulnerability has been identified in SIMATIC CFU DIQ (All versions), SIMATIC CFU PA (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.0.0), SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants) (All versions < V6.0.10), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants) (All versions), SIMATIC TDC CP51M1 (All versions), SIMATIC TDC CPU555 (All versions), SIMATIC WinAC RTX (All versions), SIMIT Simulation Platform (All versions). The PROFINET (PNIO) stack, when integrated with the Interniche IP stack, improperly handles internal resources for TCP segments where the minimum TCP-Header length is less than defined. This could allow an attacker to create a denial of service condition for TCP services on affected devices by sending specially crafted TCP segments.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-23448	<p>A vulnerability has been identified in SIMATIC Energy Manager Basic (All versions < V7.3 Update 1), SIMATIC Energy Manager PRO (All versions < V7.3 Update 1). Affected applications improperly assign permissions to critical directories and files used by the application processes. This could allow a local unprivileged attacker to achieve code execution with ADMINISTRATOR or even NT AUTHORITY/SYSTEM privileges.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-27194	<p>A vulnerability has been identified in SIMATIC PCS neo (Administration Console) (All versions < V3.1 SP1), SINETPLAN (All versions), TIA Portal (V15, V15.1, V16 and V17). The affected system cannot properly process specially crafted packets sent to port 8888/tcp. A remote attacker could exploit this vulnerability to cause a Denial-of-Service condition. The affected devices must be restarted manually.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2021-42029	<p>A vulnerability has been identified in SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 5), SIMATIC STEP 7 (TIA Portal) V17 (All versions < V17 Update 2). An attacker could achieve privilege escalation on the web server of certain devices due to improper access control vulnerability in the engineering system software. The attacker needs to have direct access to the impacted web server.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-28662	<p>A vulnerability has been identified in Simcenter Femap (All versions < V2022.1.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted .NEU files. This could allow an attacker to leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15307)</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-27837	<p>A vulnerability using PendingIntent in Accessibility prior to version 12.5.3.2 in Android R(11.0) and 13.0.1.1 in Android S(12.0) allows attacker to access the file with system privilege.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-11</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-1161	<p>An attacker with the ability to modify a user program may change user program code on some ControlLogix, CompactLogix, and GuardLogix Control systems. Studio 5000 Logix Designer writes user-readable program code to a separate location than the executed compiled code, allowing an attacker to change one and not the other.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-11</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-0999	<p>An authenticated user may be able to misuse parameters to inject arbitrary operating system commands into mySCADA myPRO versions 8.25.0 and prior.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-11</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-25794	<p>An Out-Of-Bounds Read Vulnerability in Autodesk FBX Review version 1.5.2 and prior may lead to code execution through maliciously crafted ActionScript Byte Code "ABC" files or information disclosure. ABC files are created by the Flash compiler and contain executable code. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-11</div><div>Updated: 2022-04-12</div></div>	
CVE-2021-43177	<p>As a result of an incomplete fix for CVE-2015-7225, in versions of device-two-factor prior to 4.0.2 it is possible to reuse a One-Time-Password (OTP) for one (and only one) immediately trailing interval. CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-11</div><div>Updated: 2022-04-12</div></div>	
CVE-2021-36846	<p>Authenticated (admin or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in Premio Chaty (WordPress plugin) <= 2.8.3</p>	
CVE-2022-23449	<p>A vulnerability has been identified in SIMATIC Energy Manager Basic (All versions < V7.3 Update 1), SIMATIC Energy Manager PRO (All versions < V7.3 Update 1). A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges by placing a malicious DLL in one of the directories on the DLL search path.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-23450	<p>A vulnerability has been identified in SIMATIC Energy Manager Basic (All versions < V7.3 Update 1), SIMATIC Energy Manager PRO (All versions < V7.3 Update 1). The affected system allows remote users to send maliciously crafted objects. Due to insecure deserialization of user-supplied content by the affected software, an unauthenticated attacker could exploit this vulnerability by sending a maliciously crafted serialized object. This could allow the attacker to execute arbitrary code on the device with SYSTEM privileges.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2021-40368	<p>A vulnerability has been identified in SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants) (All versions < V6.0.10), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants) (All versions < V10.1), SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants) (All versions). Affected devices improperly handle specially crafted packets sent to port 102/tcp. This could allow an attacker to create a Denial-of-Service condition. A restart is needed to restore normal operations.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-28661	<p>A vulnerability has been identified in Simcenter Femap (All versions < V2022.1.2). The affected application contains an out of bounds read past the end of an allocated buffer while parsing specially crafted .NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15114)</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-28663	<p>A vulnerability has been identified in Simcenter Femap (All versions < V2022.1.2). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted .NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15592)</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-27578	<p>An attacker can perform a privilege escalation through the SICK OEE if the application is installed in a directory where non authenticated or low privilege users can modify its content.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-11</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-22571	<p>An authenticated high privileged user can perform a stored XSS attack due to incorrect output encoding in Incapptic connect and affects all current versions.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-11</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-28346	<p>An issue was discovered in Django 2.2 before 2.2.28, 3.2 before 3.2.13, and 4.0 before 4.0.4. QuerySet.annotate(), aggregate(), and extra() methods are subject to SQL injection in column aliases via a crafted dictionary (with dictionary expansion) as the passed **kwargs.</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-12</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-27844	<p>Arbitrary File Read vulnerability in WPvivid Team Migration, Backup, Staging - WPvivid (WordPress plugin) versions <= 0.9.70</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-11</div><div>Updated: 2022-04-12</div></div>	
CVE-2022-27845	<p>Authenticated (admin or higher user role) Stored Cross-Site Scripting (XSS) in PlausibleHQ Plausible Analytics (WordPress plugin) <= 1.2.2</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-04-11</div><div>Updated: 2022-04-12</div></div>	
CVE-2021-36910	<p>Authenticated (admin user role) Stored Cross-Site Scripting (XSS) in WP-Appbox (WordPress plugin) <= 4.3.20.</p>	

	<div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>		<div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2021-36848	<div>Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Social Media Feather (WordPress plugin) versions <= 2.0.4</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2021-36896	<div>Authenticated (author or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in Pricing Table (WordPress plugin) versions <= 1.5.2</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2021-36893	<div>Authenticated (author or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in Responsive Tabs (WordPress plugin) <= 4.0.5</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2022-0835	<div>AVEVA System Platform 2020 stores sensitive information in cleartext, which may allow access to an attacker or a low-privileged user.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-25614	<div>Cross-Site Request Forgery (CSRF) in StylemixThemes eRoom - Zoom Meetings & Webinar (WordPress plugin) <= 1.3.7 allows an attacker to Sync with Zoom Meetings.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2022-25615	<div>Cross-Site Request Forgery (CSRF) in StylemixThemes eRoom - Zoom Meetings & Webinar (WordPress plugin) <= 1.3.8 allows cache deletion.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-24804	<div>Discourse is an open source platform for community discussion. In stable versions prior to 2.8.3 and beta versions prior 2.9.0.beta4 erroneously expose groups. When a group with restricted visibility has been used to set the permissions of a category, the name of the group is leaked to any user that is able to see the category. To workaround the problem, a site administrator can remove groups with restricted visibility from any category's permissions setting.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2022-27843	<div>DLL hijacking vulnerability in Kies prior to version 2.6.4.22014_2 allows attacker to execute arbitrary code.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27842	<div>DLL hijacking vulnerability in Smart Switch PC prior to version 4.2.22022_4 allows attacker to execute arbitrary code.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2022-24827	<div>Elide is a Java library that lets you stand up a GraphQL/JSON-API web service with minimal effort. When leveraging the following together: Elide Aggregation Data Store for Analytic Queries, Parameterized Columns (A column that requires a client provided parameter), and a parameterized column of type TEXT. There is the potential for a hacker to provide a carefully crafted query that would bypass server side authorization filters through SQL injection. A recent patch to Elide 6.1.2 allowed the '-' character to be included in parameterized TEXT columns. This character can be interpreted as SQL comments ('--') and allow the attacker to remove the WHERE clause from the generated query and bypass authorization filters. A fix is provided in Elide 6.1.4. The vulnerability only exists for parameterized columns of type TEXT and only for analytic queries (CRUD is not impacted). Workarounds include leveraging a different type of parameterized column (TIME, MONEY, etc) or not leveraging parameterized columns.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-24829	<div>Garden is an automation platform for Kubernetes development and testing. In versions prior to 0.12.39 multiple endpoints did not require authentication. In some operating modes this allows for an attacker to gain access to the application erroneously. The configuration is leaked through the /api endpoint on the local server that is responsible for serving the Garden dashboard. At the moment, this server is accessible to 0.0.0.0 which makes it accessible to anyone on the same network (or anyone on the internet if they are on a public, static IP). This may lead to the ability to compromise credentials, secrets or environment variables. Users are advised to upgrade to version 0.12.39 as soon as possible. Users unable to upgrade should use a firewall blocking access to port 9777 from all untrusted network machines.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2022-24832	<div>GoCD is an open source a continuous delivery server. The bundled gocd-ldap-authentication-plugin included with the GoCD Server fails to correctly escape special characters when using the username to construct LDAP queries. While this does not directly allow arbitrary LDAP data exfiltration, it can allow an existing LDAP-authenticated GoCD user with malicious intent to construct and execute malicious queries, allowing them to deduce facts about other users or entries within the LDAP database (e.g alternate fields, usernames, hashed passwords etc) through brute force mechanisms. This only affects users who have a working LDAP authorization configuration enabled on their GoCD server, and only is exploitable by users authenticating using such an LDAP configuration. This issue has been fixed in GoCD 22.1.0, which is bundled with gocd-ldap-authentication-plugin v2.2.0-144.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27568	<div>Heap-based buffer overflow vulnerability in parser_iloc function in libsimba library prior to SMR Apr-2022 Release 1 allows code execution by remote attacker.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2022-27569	<div>Heap-based buffer overflow vulnerability in parser_infe function in libsimba library prior to SMR Apr-2022 Release 1 allows code execution by remote attacker.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27572	<div>Heap-based buffer overflow vulnerability in parser_ipma function of libsimba library prior to SMR Apr-2022 Release 1 allows code execution by remote attackers.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2022-27570	<div>Heap-based buffer overflow vulnerability in parser_single_iref function in libsimba library prior to SMR Apr-2022 Release 1 allows code execution by remote attacker.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-26098	<div>Heap-based buffer overflow vulnerability in sheifd_create function of libsimba library prior to SMR Apr-2022 Release 1 allows code execution by remote attackers.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2022-27571	<div>Heap-based buffer overflow vulnerability in sheifd_get_info_image function in libsimba library prior to SMR Apr-2022 Release 1 allows code execution by remote attacker.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-24837	<div>HedgeDoc is an open-source, web-based, self-hosted, collaborative markdown editor. Images uploaded with HedgeDoc version 1.9.1 and later have an enumerable filename after the upload, resulting in potential information leakage of uploaded documents. This is especially relevant for private notes and affects all upload backends, except Lutim and imgur. This issue is patched in version 1.9.3 by replacing the filename generation with UUIDv4. If you cannot upgrade to HedgeDoc 1.9.3, it is possible to block POST requests to `/uploadimage`, which will disable future uploads.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2022-27836	<div>Improper access control and path traversal vulnerability in StroageManager and StroageManagerService prior to SMR Apr-2022 Release 1 allow local attackers to access arbitrary system files without a proper permission.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-1193	<div>Improper access control in GitLab CE/EE versions 10.7 prior to 14.7.7, 10.8 prior to 14.8.5, and 10.9 prior to 14.9.2 allows a malicious actor to obtain details of the latest commit in a private project via Merge Requests under certain circumstances</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>	CVE-2022-27838	<div>Improper access control vulnerability in FactoryCamera prior to version 2.1.96 allows attacker to access the file with system privilege.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-28776	<div>Improper access control vulnerability in Galaxy Store prior to version 4.5.36.4 allows attacker to install applications from Galaxy Store without user interactions.</div>	CVE-2022-26091	<div>Improper access control vulnerability in Knox Manage prior to SMR Apr-2022 Release 1 allows that physical attackers can bypass Knox Manage using a function key of hardware keyboard.</div>

	<div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-25831	<div>Improper access control vulnerability in S Secure prior to SMR Apr-2022 Release 1 allows physical attackers to access secured data in certain conditions.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-28777	<div>Improper access control vulnerability in Samsung Members prior to version 13.6.08.5 allows local attacker to execute call function without CALL_PHONE permission.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-26090	<div>Improper access control vulnerability in SamsungContacts prior to SMR Apr-2022 Release 1 allows that attackers can access contact information without permission.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-25833	<div>Improper authentication in ImsService prior to SMR Apr-2022 Release 1 allows attackers to get IMSI without READ_PRIVILEGED_PHONE_STATE permission.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27839	<div>Improper authentication vulnerability in SecretMode in Samsung Internet prior to version 16.2.1 allows attackers to access bookmark tab without proper credentials.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-26092	<div>Improper boundary check in Quram Agif library prior to SMR Apr-2022 Release 1 allows arbitrary code execution.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27831	<div>Improper boundary check in sflvd_rdbuf_bits of libslvextractor prior to SMR Apr-2022 Release 1 allows attackers to read out of bounds memory.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27841	<div>Improper exception handling in Samsung Pass prior to version 3.7.07.5 allows physical attacker to view the screen that is previously running without authentication</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27574	<div>Improper input validation vulnerability in parser_iloc and sheifd_find_itemIndexin fuctions of libsimba library prior to SMR Apr-2022 Release 1 allows out of bounds write by privileged attacker.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-28542	<div>Improper sanitization of incoming intent in Galaxy Store prior to version 4.5.40.5 allows local attackers to access privileged content providers as Galaxy Store permission.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27823	<div>Improper size check in sapefd_parse_meta_HEADER old function of libsapeextractor library prior to SMR Apr-2022 Release 1 allows out of bounds read via a crafted media file.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27827	<div>Improper validation vulnerability in MediaMonitorDimension prior to SMR Apr-2022 Release 1 allows attackers to launch certain activities.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27830	<div>Improper validation vulnerability in SemBlurInfo prior to SMR Apr-2022 Release 1 allows attackers to launch certain activities.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27829	<div>Improper validation vulnerability in VerifyCredentialResponse prior to SMR Apr-2022 Release 1 allows attackers to launch certain activities.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-20066	<div>In atf (hwfde), there is a possible leak of sensitive information due to incorrect error handling. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171729; Issue ID: ALPS06171729.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-20064	<div>In cccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-20071	<div>In ccu, there is a possible escalation of privilege due to a missing</div>

	<div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-28775	<div>Improper access control vulnerability in Samsung Flow prior to version 4.8.06.5 allows attacker to write the file without Samsung Flow permission.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-28778	<div>Improper access control vulnerability in Samsung Security Supporter prior to version 1.2.40.0 allows attacker to set the arbitrary folder as Secret Folder without Samsung Security Supporter permission</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27840	<div>Improper access control vulnerability in SamsungRecovery prior to version 8.1.43.0 allows local attckers to delete arbitrary files as SamsungRecovery permission.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-25832	<div>Improper authentication vulnerability in S Secure prior to SMR Apr-2022 Release 1 allows physical attackers to use locked Myfiles app without authentication.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27832	<div>Improper boundary check in media.extractor library prior to SMR Apr-2022 Release 1 allows attackers to cause denial of service via a crafted media file.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27821	<div>Improper boundary check in Quram Agif library prior to SMR Apr-2022 Release 1 allows attackers to cause denial of service via crafted image file.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27835	<div>Improper boundary check in UWB firmware prior to SMR Apr-2022 Release 1 allows arbitrary memory write.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27833	<div>Improper input validation in DSP driver prior to SMR Apr-2022 Release 1 allows out-of-bounds write by integer overflow.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27573	<div>Improper input validation vulnerability in parser_infe and sheifd_find_itemIndexin fuctions of libsimba library prior to SMR Apr-2022 Release 1 allows out of bounds write by privileged attackers.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27825	<div>Improper size check in sapefd_parse_meta_HEADER function of libsapeextractor library prior to SMR Apr-2022 Release 1 allows out of bounds read via a crafted media file.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27824	<div>Improper size check of in sapefd_parse_meta_DESCRIPTION function of libsapeextractor library prior to SMR Apr-2022 Release 1 allows out of bounds read via a crafted media file</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27828	<div>Improper validation vulnerability in MediaMonitorEvent prior to SMR Apr-2022 Release 1 allows attackers to launch certain activities.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-27826	<div>Improper validation vulnerability in SemSuspendDialogInfo prior to SMR Apr-2022 Release 1 allows attackers to launch certain activities.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-20081	<div>In A-GPS, there is a possible man in the middle attack due to improper certificate validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06461919; Issue ID: ALPS06461919.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-20063	<div>In atf (spm), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06171715; Issue ID: ALPS06171715.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>
CVE-2022-20065	<div>In cccci, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108658; Issue ID: ALPS06108658.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-04-11 Updated: 2022-04-12</div>

	<p>certificate validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06183315; Issue ID: ALPS06183315.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-20076</p> <p>In ged, there is a possible memory corruption due to an incorrect error handling. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05838808; Issue ID: ALPS05839556.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-20075	<p>In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05838808; Issue ID: ALPS05838808.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-20052</p> <p>In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-20062	<p>In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-20067</p> <p>In mdp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836585; Issue ID: ALPS05836585.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-20068	<p>In mobile_log_d, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308907; Issue ID: ALPS06308907.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-20074</p> <p>In preloader (partition), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06183301; Issue ID: ALPS06183301.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-20073	<p>In preloader (usb), there is a possible out of bounds write due to a integer underflow. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160841; Issue ID: ALPS06160841.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-20069</p> <p>In preloader (usb), there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160425; Issue ID: ALPS06160425.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-20072	<p>In search engine service, there is a possible way to change the default search engine due to an incorrect comparison. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06219118; Issue ID: ALPS06219118.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-20070</p> <p>In ssmr, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06362920; Issue ID: ALPS06362920.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-20080	<p>In SUB2AF, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05881290; Issue ID: ALPS05881290.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-1302</p> <p>In the MZ Automation LibIEC61850 in versions prior to 1.5.1 an unauthenticated attacker can craft a goose message, which may result in a denial of service.</p> <div>UNRATEDVector: unkownCreated: 2022-04-12Updated: 2022-04-12</div>
CVE-2022-20077	<p>In vow, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05837742; Issue ID: ALPS05852812.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-20078</p> <p>In vow, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05852819; Issue ID: ALPS05852819.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-20079	<p>In vow, there is a possible read of uninitialized data due to a improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05837742; Issue ID: ALPS05857289.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-27575</p> <p>Information exposure vulnerability in One UI Home prior to SMR April-2022 Release 1 allows to access currently launched foreground app information without permission.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-27822	<p>Information exposure vulnerability in ril property setting prior to SMR April-2022 Release 1 allows access to EF_RUIMID value without permission.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-27576</p> <p>Information exposure vulnerability in Samsung DeX Home prior to SMR April-2022 Release 1 allows to access currently launched foreground app information without permission</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-24815	<p>JHipster is a development platform to quickly generate, develop, & deploy modern web applications & microservice architectures. SQL Injection vulnerability in entities for applications generated with the option "reactive with Spring WebFlux" enabled and an SQL database using r2dbc. Applications created without "reactive with Spring WebFlux" and applications with NoSQL databases are not affected. Users who have generated a microservice Gateway using the affected version may be impacted as Gateways are reactive by default. Currently, SQL injection is possible in the findAllBy(Pageable pageable, Criteria criteria) method of an entity repository class generated in these applications as the where clause using Criteria for queries are not sanitized and user input is passed on as it is by the criteria. This issue has been patched in v7.8.1. Users unable to upgrade should be careful when combining criterias and conditions as the root of the issue lies in the EntityManager.java class when creating the where clause via Conditions.just(criteria.toString()). `just` accepts the literal string provided. Criteria's `toString` method returns a plain string and this combination is vulnerable to sql injection as the string is not sanitized and will contain whatever used passed as input using any plain SQL.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-1157</p> <p>Missing sanitization of logged exception messages in all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 of GitLab CE/EE causes potential sensitive values in invalid URLs to be logged</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-1067	<p>Navigating to a specific URL with a patient ID number will result in the server generating a PDF of a lab report without authentication and rate limiting.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>	<p>CVE-2022-24838</p> <p>Nextcloud Calendar is a calendar application for the nextcloud framework. SMTP Command Injection in Appointment Emails via Newlines: as newlines and special characters are not sanitized in the email value in the JSON request, a malicious attacker can inject newlines to break out of the `RCPT TO:` SMTP command and begin injecting arbitrary SMTP commands. It is recommended that Calendar is upgraded to 3.2.2. There are no workaround available.</p> <div>UNRATEDVector: unkownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-24836	<p>Nokogiri is an open source XML and HTML library for Ruby. Nokogiri `<code>< v1.13.4` contains an inefficient regular expression that is susceptible</code></p>	<p>CVE-2022-26094</p> <p>Null pointer dereference vulnerability in parser_auxC function in</p>

	<div>to excessive backtracking when attempting to detect encoding in HTML documents. Users are advised to upgrade to Nokogiri `>= 1.13.4`. There are no known workarounds for this issue.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	<div>libsimba library prior to SMR Apr-2022 Release 1 allows out of bounds write by remote attacker.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-26095	<div>Null pointer dereference vulnerability in parser_colr function in libsimba library prior to SMR Apr-2022 Release 1 allows out of bounds write by remote attacker.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-27567 <div>Null pointer dereference vulnerability in parser_hvcC function of libsimba library prior to SMR Apr-2022 Release 1 allows out of bounds write by remote attackers.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-26099	<div>Null pointer dereference vulnerability in parser_infe function of libsimba library prior to SMR Apr-2022 Release 1 allows out of bounds read by remote attackers.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-26093 <div>Null pointer dereference vulnerability in parser_irot function in libsimba library prior to SMR Apr-2022 Release 1 allows out of bounds write by remote attacker.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-26096	<div>Null pointer dereference vulnerability in parser_ispe function in libsimba library prior to SMR Apr-2022 Release 1 allows out of bounds write by remote attacker.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-26097 <div>Null pointer dereference vulnerability in parser_unknown_property function in libsimba library prior to SMR Apr-2022 Release 1 allows out of bounds write by remote attacker.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-24839	<div>org.cyberneko.html is an html parser written in Java. The fork of `org.cyberneko.html` used by Nokogiri (Rubygem) raises a `java.lang.OutOfMemoryError` exception when parsing ill-formed HTML markup. Users are advised to upgrade to `>= 1.9.22.noko2`. Note: The upstream library `org.cyberneko.html` is no longer maintained. Nokogiri uses its own fork of this library located at https://github.com/sparklemotion/nekohtml and this CVE applies only to that fork. Other forks of nekohtml may have a similar vulnerability.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-28543 <div>Path traversal vulnerability in Samsung Flow prior to version 4.8.07.4 allows local attackers to read arbitrary files as Samsung Flow permission.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-28544	<div>Path traversal vulnerability in unzip method of InstallAgentCommonHelper in Galaxy store prior to version 4.5.40.5 allows attacker to access the file of Galaxy store.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-24833 <div>PrivateBin is minimalist, open source online pastebin clone where the server has zero knowledge of pasted data. In PrivateBin < v1.4.0 a cross-site scripting (XSS) vulnerability was found. The vulnerability is present in all versions from v0.21 of the project, which was at the time still called ZeroBin. The issue is caused by the fact that SVGs can contain JavaScript. This can allow an attacker to execute code, if the user opens a paste with a specifically crafted SVG attachment, and interacts with the preview image and the instance isn't protected by an appropriate content security policy. Users are advised to either upgrade to version 1.4.0 or to ensure the content security policy of their instance is set correctly.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-22255	<div>The application framework has a common DoS vulnerability.Successful exploitation of this vulnerability may affect the availability.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2021-40065 <div>The communication module has a service logic error vulnerability.Successful exploitation of this vulnerability may affect data confidentiality.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-22257	<div>The customization framework has a vulnerability of improper permission control.Successful exploitation of this vulnerability may affect data integrity.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2021-46740 <div>The device authentication service module has a defect vulnerability introduced in the design process.Successful exploitation of this vulnerability may affect data confidentiality.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-22253	<div>The DFX module has a vulnerability of improper validation of integrity check values.Successful exploitation of this vulnerability may affect system stability.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-22256 <div>The DFX module has an access control vulnerability.Successful exploitation of this vulnerability may affect data confidentiality.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2021-46742	<div>The multi-window module has a vulnerability of unauthorized insertion and tampering of Settings.Secure data.Successful exploitation of this vulnerability may affect the availability.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-29080 <div>The npm-dependency-versions package through 0.3.0 for Node.js allows command injection if an attacker is able to call dependencyVersions with a JSON object in which pkgs is a key, and there are shell metacharacters in a value.</div> <div>UNRATEDVector: unknownCreated: 2022-04-12Updated: 2022-04-12</div>
CVE-2021-4047	<div>The release of OpenShift 4.9.6 included four CVE fixes for the haproxy package, however the patch for CVE-2021-39242 was missing. This issue only affects Red Hat OpenShift 4.9.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2021-22055 <div>The SchedulerServer in Vmware photon allows remote attackers to inject logs through r in the package parameter. Attackers can also insert malicious data and fake entries.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-27577	<div>The vulnerability in the MSC800 in all versions before 4.15 allows for an attacker to predict the TCP initial sequence number. When the TCP sequence is predictable, an attacker can send packets that are forged to appear to come from a trusted computer. These forged packets could compromise services on the MSC800. SICK has released a new firmware version of the SICK MSC800 and recommends updating to the newest version.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-22258 <div>The Wi-Fi module has an event notification vulnerability.Successful exploitation of this vulnerability may allow third-party applications to intercept event notifications and add information and result in elevation-of-privilege.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2021-38125	<div>Unauthenticated remote code execution in Micro Focus Operations Bridge containerized, affecting versions 2021.05, 2021.08, and newer versions of Micro Focus Operations Bridge containerized if the deployment was upgraded from 2021.05 or 2021.08. The vulnerability could be exploited to unauthenticated remote code execution.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-28779 <div>Uncontrolled search path element vulnerability in Samsung Android USB Driver windows installer program prior to version 1.7.50 allows attacker to execute arbitrary code.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-28541	<div>Uncontrolled search path element vulnerability in Samsung Update prior to version 3.0.77.0 allows attackers to execute arbitrary code as Samsung Update permission.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-27834 <div>Use after free vulnerability in dsp_context_unload_graph function of DSP driver prior to SMR Apr-2022 Release 1 allows attackers to perform malicious actions.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>

CVE-2022-22962	VMware Horizon Client for Linux (prior to 22.x) contains a local privilege escalation as a user is able to change the default shared folder location due to a vulnerable symbolic link. Successful exploitation can result in linking to a root owned file. <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-22964	VMware Horizon Client for Linux (prior to 22.x) contains a local privilege escalation that allows a user to escalate to root due to a vulnerable configuration file. <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>
CVE-2022-22954	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability due to server-side template injection. A malicious actor with network access can trigger a server-side template injection that may result in remote code execution. <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>	CVE-2022-1316	ZeroTierOne for windows local privilege escalation because of incorrect directory privilege in GitHub repository zerotier/zerotierone prior to 1.8.8. Local Privilege Escalation <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-12</div>

Source: [Hybrid Analysis](#)

Top malicious files

100% Threat score	App_software.exe	100% Threat score	PQfWInstall64_4.6.270.exe
100% Threat score	freevpn_setup.exe	100% Threat score	Chomp SMS v8.54 b9085401 (Pro) (Lite Mod).apk
100% Threat score	tmp_mf8yaqr	100% Threat score	tmpw09gmsa7
100% Threat score	7b2449bb8be1b37a9d580c2592a67a759a3116fe640041d0f36dc93ca3db4487	100% Threat score	28.msi
100% Threat score	DPT_4.00.10_TSW_9.00.10_PM_5.00.10-201842.4a.exe	97% Threat score	meterpreter.dll
85% Threat score	FORCEPOINT-ONE-ENDPOINT-x64.exe	83% Threat score	Invoice FW76857484.html
82% Threat score	Arrival Notice.xlsx	75% Threat score	abcd.xls











Source: [Hybrid Analysis](#)

Top malicious URL

97% Threat score	http://27.215.177.182:35331/bin.sh	93% Threat score	http://222.142.212.239:49978/Mozi.m
91% Threat score	http://221.15.171.42:54409/Mozi.m	91% Threat score	http://222.141.89.158:34526/Mozi.m
85% Threat score	https://tele-ui-899109287.onrender.com/	81% Threat score	https://bold-unit-9060.wafidoy7421238.workers.dev/&data=04%7C01%7Ccagliari@inail.it%7C3ff534050a844597140
80% Threat score	http://www.hollywellprojectmanagement.co.uk/	80% Threat score	http://anova.co/
75% Threat score	http://38dca5e26bb54db09f34d1ecefaf7f75.cell0.alpha.uidwifi.com/	75% Threat score	http://snip.ly/ujqn9a
75% Threat score	http://www.eztechit.com/	73% Threat score	https://t.co/2ZONaJWNs6



Source: [SpamHaus](#)








Top spamming countries

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











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 Michael Persaud Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.
	#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 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.
	#7 RR Media A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.		#8 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.
	#9 Richpro Trade Inc. / Richvestor GmbH Uses botnets or hires botnet spammers to send spam linking back to suspect investment, "quack-health-cures" and other sites that he owns or is an affiliate of. Botnet spamming and hosting sites on hacked servers is fully criminal in much of the world. Managed or owned by a Timo Richert.		

Source: [SpamHaus](#)

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

Source: [SpamHaus](#)




Top phishing countries			
	#1 United States		#2 Russia
	#3 Germany		#4 Japan
	#5 Singapore		#6 Netherlands
	#7 France		#8 Australia
	#9 India		#10 Hong Kong

Source: [Have I been pwned?](#)



Have I been pwnd

Nothing today

Source: [Imperva DDOS Map](#)

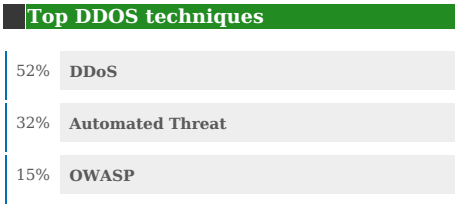
Top DDOS attackers	
	United States (34%)
	Germany (12%)
	Netherlands (9%)

Source: [Imperva DDOS Map](#)

Top DDOS country targets	
	Russia (36%)
	United States (24%)



Source: [Imperva DDOS Map](#)



Source: [Imperva DDOS Map](#)

