



## Your Security Rabbits report for February 10, 2022

### Hot topics

Nothing today

### News



**2021 was the most prolific year on record for data breaches**  
2021 was the most prolific year on record for data breaches, surpassing 2017's all-time high. A total of 1,862 data compromises were reported by U.S. organizations--a 68 percent increase over 2020.



**AA22-040A: 2021 Trends Show Increased Globalized Threat of Ransomware**  
Immediate Actions You Can Take Now to Protect Against Ransomware: \* Update your operating system and software. \* Implement user training and phishing exercises to raise awareness about the risk of suspicious links and attachments. \* If you use Remote Desktop Protocol (RDP), secure and monitor it. \* Make an offline backup of your data. \* Use multifactor authentication (MFA). In 2021, cybersecurity authorities in the United States,[1][2][3] Australia,[4] and the United Kingdom[5] observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally. The Federal Bureau of Investigation (FBI), the Cybersecurit[...]



**CISA, FBI, NSA Issue Advisory on Severe Increase in Ransomware Attacks**  
Cybersecurity authorities from Australia, the U.K., and the U.S. have published a joint advisory warning of an increase in sophisticated, high-impact ransomware attacks targeting critical infrastructure organizations across the world in 2021. The incidents singled out a broad range of sectors, including defense, emergency services, agriculture, government facilities, IT, healthcare, financial



**Critical RCE Flaws in 'PHP Everywhere' Plugin Affect Thousands of WordPress Sites**  
Critical security vulnerabilities have been disclosed in a WordPress plugin known as PHP Everywhere that's used by more than 30,000 websites worldwide and could be abused by an attacker to execute arbitrary code on affected systems. PHP Everywhere is used to flip the switch on PHP code across WordPress installations, enabling users to insert and execute PHP-based code in the content management



**Cybercriminals Swarm Windows Utility Regsvr32 to Spread Malware**  
The living-off-the-land binary (LOLBin) is anchoring a rash of cyberattacks bent on evading security detection to drop Qbot and Lokibot.



**ESET Threat Report T3 2021**  
A view of the T3 2021 threat landscape as seen by ESET telemetry and from the perspective of ESET threat detection and research experts The post ESET Threat Report T3 2021 appeared first on WeLiveSecurity



**FBI Received 1,600 SIM Swapping Complaints in 2021**  
The Federal Bureau of Investigation (FBI) this week announced that between 2018 and 2021 its Internet Crime Complaint Center (IC3) received more than 1,900 complaints related to SIM swapping.



**Guide: Alert Overload and Handling for Lean IT Security Teams**  
Alarming research reveals the stress and strains the average cybersecurity team experiences on a daily basis. As many as 70% of teams report feeling emotionally overwhelmed by security alerts. Those alerts come at such high volume, high velocity, and high intensity that they become an extreme source of stress. So extreme, in fact, that people's home lives are negatively affected. Alert overload



**MageCart attacks hit hundreds of outdated Magento sites**  
Analysts at Sansec found the source of over 500-e-commerce stores involving a single domain loading a credit card skimmer on all of them. The attack became evident in late January when a Sansec crawler discovered 374 infections in one day, all using the same malware. The domain that loaded the malware, naturalfreshmall[.]com, is currently offline [...] The post MageCart attacks hit hundreds of outdated Magento sites appeared first on IT Security Guru.



**3 Tips for Facing the Harsh Truths of Cybersecurity in 2022, Part I**  
Sonya Duffin, ransomware and data-protection expert at Veritas Technologies, shares three steps organizations can take today to reduce cyberattack fallout.



**CISA warns to address SAP ICMAD flaw immediately**  
The US CISA warns to address a severe security vulnerability dubbed ICMAD impacting SAP business apps using ICM.. Internet Communication Manager Advanced Desync (ICMAD) is a memory pipes (MPI) desynchronization vulnerability tracked as CVE-2022-22536. An unauthenticated remote attacker could exploit this issue by sending a simple HTTP request to a vulnerable instance and take over it. [...] The post CISA warns to address SAP ICMAD flaw immediately appeared first on Security Affairs.



**COVID-19 news fuels rise in domain-related cybercrime, report says**  
Data confirm that hackers leveraged the global pandemic for financial gain, a particular risk to healthcare entities given brand abuse and patient privacy or misinformation risk.



**Critical RCE flaws in PHP Everywhere WordPress plugin affect thousands of sites**  
WordPress plugin PHP Everywhere is affected by three critical issues that can be exploited to execute arbitrary code on affected systems. Wordfence experts found three critical remote code execution vulnerabilities in the PHP Everywhere WordPress plugin, all the issues have received a CVSS score of 9.9. The plugin that allows WordPress admins to insert PHP code [...] The post Critical RCE flaws in PHP Everywhere WordPress plugin affect thousands of sites appeared first on Security Affairs.



**Cyware Enhances Automated Threat Intelligence Sharing for Auto-ISAC to Promote a Proactive, Collective Defense**  
Cyware today announced that it has partnered with the Auto-ISAC to give its members the ability to automatically aggregate, share, and collaborate on actionable threat intelligence.



**Ex-Gumshoe Nabs Cybercrooks with FBI Tactics**  
Crane Hassold, former FBI analyst turned director of threat intel at Abnormal Security, shares stories from his covert work with cyberattackers.























**Google February 2022 Android security updates fix remote escalation bug**  
Google February 2022 Android security updates address two critical flaws, including a remote escalation of privilege. Google has released the February 2022 Android security updates that address two critical vulnerabilities, one of them is a remote escalation of privilege that requires no user interaction for its exploitation. The vulnerability, tracked as CVE-2021-39675, only affects the System [...] The post Google February 2022 Android security updates fix remote escalation bug appeared first on Security Affairs.



**Iranian Hackers Using New Marlin Backdoor in 'Out to Sea' Espionage Campaign**  
An advanced persistent threat (APT) group with ties to Iran has refreshed its malware toolset to include a new backdoor dubbed Marlin as part of a long-running espionage campaign that started in April 2018. Slovak cybersecurity company ESET attributed the attacks -- codenamed "Out to Sea" -- to a threat actor called OilRig (aka APT34), while also conclusively connecting its activities to a second



**Master decryption keys for Maze, Egregor, and Sekhmet ransomware leaked online**  
The master decryption keys for the Maze, Egregor, and Sekhmet ransomware operations were released last night on the BleepingComputer forums. The master decryption keys for the Maze, Egregor, and Sekhmet ransomware families were released on the BleepingComputer forums by the alleged malware developer. The Maze group was considered one of the most prominent ransomware operations [...] The post Master decryption keys for Maze, Egregor, and Sekhmet ransomware leaked online appeared first on Security Affairs.

 <p>CYWARE SOCIAL Cyware News - Latest Cyber News</p>	<p><b>Microsoft 365 Phishing Attack Makes Comeback</b></p> <p>According to cybersecurity researchers at Vade, malicious actors are dusting off Right-to-Left Override (RLO) attacks to trick victims into executing files with disguised extensions.</p>	 <p>Security Affairs</p>	<p><b>Microsoft February 2022 Patch Tuesday security updates fix a zero-day</b></p> <p>Microsoft February 2022 Patch Tuesday security updates addressed 51 flaws in multiple products, including a zero-day bug. Microsoft February 2022 Patch Tuesday security updates addressed 51 flaws in multiple products including Microsoft Windows and Windows Components, Azure Data Explorer, Kestrel Web Server, Microsoft Edge (Chromium-based), Windows Codecs Library, Microsoft Dynamics, Microsoft Dynamics GP, Microsoft Office [...] The post Microsoft February 2022 Patch Tuesday security updates fix a zero-day appeared first on Security Affairs.</p>
 <p>Threatpost</p>	<p><b>MoleRats APT Flaunts New Trojan in Latest Cyberespionage Campaign</b></p> <p>Researchers from Proofpoint have spotted a new Middle East-targeted phishing campaign that delivers a novel malware dubbed NimbleMamba.</p>	 <p>CyberScoop</p>	<p><b>Overcoming key business and operational challenges with XDR</b></p> <p>Improving detection of advanced cyberthreats is a high priority in any security operation. However, a lack of visibility in an ever-expanding attack surface coupled with too many siloed security tools can overwhelm security teams with alerts and false positives. In addition, investigating broader malicious operations requires a complex workflow and staffing with domain expertise, a new report says. According to security experts at Cybereason, extended detection and response (XDR) provides security analysts with better visibility into the attack surface and the ability to act quickly across multiple security layers. They recently released a guide to help practitioners better understand AI-dri[...]</p>
 <p>ZDNet   security RSS</p>	<p><b>PHP Everywhere code execution bugs impact thousands of WordPress websites</b></p> <p>The remote code execution flaws are of critical severity.</p>	 <p>CYWARE SOCIAL Cyware News - Latest Cyber News</p>	<p><b>Preventing software security vulnerabilities with automation</b></p> <p>A team of UTSA researchers is exploring how a new automated approach could prevent software security vulnerabilities. They developed a deep learning model to extract security policies automatically.</p>
 <p>CYWARE SOCIAL Cyware News - Latest Cyber News</p>	<p><b>Ransomware dev releases Egregor, Maze master decryption keys</b></p> <p>The master decryption keys for the Maze, Egregor, and Sekhmet ransomware operations were released last night on the BleepingComputer forums by the alleged malware developer.</p>	 <p>IT Security Guru</p>	<p><b>Rapper accused of laundering billions worth of bitcoin</b></p> <p>A TikTok rapper and her husband have been charged with conspiring to launder \$4.5bn worth of bitcoin. The bitcoin was stolen from a virtual currency exchange in 2016 in the biggest crypto-heist the world has ever seen. Heather Morgan, 31, and Ilya' Dutch' Lichtenstein, 34, both of New York, New York, were arrested in Manhattan on [...] The post Rapper accused of laundering billions worth of bitcoin appeared first on IT Security Guru.</p>
 <p>The Hacker News</p>	<p><b>Russia Cracks Down on 4 Dark Web Marketplaces for Stolen Credit Cards</b></p> <p>A special law enforcement operation undertaken by Russia has led to the seizure and shutdown of four online bazaars that specialized in the theft and sales of stolen credit cards, as the government continues to take active measures against harboring cybercriminals on its territory. To that end, the domains operated by the card fraud forms and marketplaces, Ferum Shop, Sky-Fraud, Trump's Dumps,</p>	 <p>Krebs on Security</p>	<p><b>Russian Govt. Continues Carding Shop Crackdown</b></p> <p>Russian authorities have arrested six men accused of operating some of the most active online bazaars for selling stolen payment card data. The crackdown -- the second closure of major card fraud shops by Russian authorities in as many weeks -- comes closely behind Russia's arrest of 14 alleged affiliates of the REvil ransomware gang, and has many in the cybercrime underground asking who might be next.</p>
 <p>SOPHOS Naked Security</p>	<p><b>S3 Ep69: WordPress woes, Wormhole holes, and a Microsoft change of heart [Podcast + Transcript]</b></p> <p>Latest episode - listen now!</p>	 <p>IT Security Guru</p>	<p><b>Safer Internet Day 2022 - How Can The Online World Be A Safer Place?</b></p> <p>The 8th of February marked the 19th Safer Internet Day which saw over 200 countries take a collaborative stance to make the Internet a safer and better place for all, particularly for younger people. Over the past 18 months, online activity sky-rocketed due to the disruptions caused by the pandemic. With many faced with lockdowns, [...] The post Safer Internet Day 2022 - How Can The Online World Be A Safer Place? appeared first on IT Security Guru.</p>
 <p>CyberScoop</p>	<p><b>SEC's breach notification proposal one step closer to a final vote</b></p> <p>The Securities and Exchange Commission voted Wednesday 3-1 to approve a recommendation for tighter mandatory cybersecurity requirements for financial institutions. The proposed rule will now open to public comment before a final vote. "The proposed rules and amendments are designed to enhance cybersecurity preparedness and could improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks," SEC Chairman Gary Gensler said at the agency's open meeting. Most critically, the new rule would require confidential reports of any "significant" cybersecurity incidents to the SEC within 48 hours. The proposal also would require advisers and funds to ado[...]</p>	 <p>SOPHOS Naked Security</p>	<p><b>Self-styled "Crocodile of Wall Street" arrested with husband over Bitcoin megaheist</b></p> <p>The cops say they've recovered 80% of a \$72 million cryptocurrency heist... but the recovered funds alone are now worth over \$4 billion!</p>
 <p>CYWARE SOCIAL Cyware News - Latest Cyber News</p>	<p><b>Siemens, Schneider Electric Address Nearly 50 ICS Vulnerabilities</b></p> <p>Industrial equipment giants Siemens and Schneider Electric released a total of 15 advisories on Tuesday to address nearly 50 vulnerabilities discovered in their products.</p>	 <p>CYWARE SOCIAL Cyware News - Latest Cyber News</p>	<p><b>StellarParticle Campaign - New Undetected Malware Revealed After Two Years</b></p> <p>Hackers associated with SolarWind attacks have been using two new threats, the GoldMax backdoor and the TrailBlazer malware family, in StellarParticle campaigns for over two years. Researchers have provided detailed information regarding the latest TTPs observed in cyberattacks and suggested organizations to implement a multi-layered defense strategy to stay protected.</p>
 <p>The Hacker News</p>	<p><b>U.S. Arrests Two and Seizes \$3.6 Billion Cryptocurrency Stolen in 2016 Bitfinex Hack</b></p> <p>The U.S. Justice Department (DoJ) on Tuesday announced the arrest of a married couple in connection with conspiring to launder cryptocurrency worth \$4.5 billion that was siphoned during the hack of the virtual currency exchange Bitfinex in 2016. Ilya Lichtenstein, 34, and his wife, Heather Morgan, 31, both of New York, are alleged to have "stolen funds through a labyrinth of cryptocurrency</p>	 <p>Security Affairs</p>	<p><b>US citizens lost more than \$68M to SIM swap attacks in 2021, FBI warns</b></p> <p>The Federal Bureau of Investigation (FBI) warns of an escalation in SIM swap attacks that caused millions of losses. The Federal Bureau of Investigation (FBI) observed an escalation in SIM swap attacks aimed at stealing millions from the victims by hijacking their mobile phone numbers. The FBI reported that US citizens have lost more than [...] The post US citizens lost more than \$68M to SIM swap attacks in 2021, FBI warns appeared first on Security Affairs.</p>
 <p>CYWARE SOCIAL Cyware News - Latest Cyber News</p>	<p><b>Watch Out! Pay-Per-Install PrivateLoader Malware Distribution Service is Flourishing</b></p> <p>Intel 471 studied the Pay-Per-Install service offered by PrivateLoader to expand their target and shed light on the deployment of popular malware strains, including Smokeloader and Vidar. The low cost, easy access of such services inspired more cybercriminals to expand their attack horizons. More experts should watch this space if they wish to develop countermeasures.</p>	 <p>CYWARE SOCIAL Cyware News - Latest Cyber News</p>	<p><b>Zerodium Offers Huge Money for Zero-day Exploits</b></p> <p>Premium exploits acquisition platform Zerodium rolled out an offer of \$400,000 in bounty rewards to anyone who reports an RCE zero-day vulnerability in Outlook. It is reportedly a temporary offer. It is offering up to \$200,000 for exploits leading to remote code execution in Mozilla Thunderbird. Security teams in various organizations must watch out for zero-days because such a bug in Microsoft Outlook can have an unimaginable impact.</p>

## Twitter

 <p>Wolfgang Sesin</p>	<p>New post from (CVE-2021-25992) has been published on</p>	 <p>www.sesin.at</p>	<p>New post from (CVE-2021-25992) has been published on</p>
<p>NEW: CVE-2021-25992 In Ifme, versions 1.0.0 to v.7.33.2 dont properly invalidate a users session even after the user initiated logout. It makes it possible for an</p>		<p>CVE-2021-25992 : In Ifme, versions 1.0.0 to v.7.33.2 dont properly invalidate a</p>	

	attacker to reuse the admin cookies either vi... (click for more) Severity: CRITICAL		users session even after the user initiated logout. It makes it possible for an attacker to reuse the admin cookies either via local/network access or by o...
Threat Intel Center		CVE.report	

Source: NIST

NIST CVE: Critical

CVE-2021-25992	In Ifme, versions 1.0.0 to v.7.33.2 don't properly invalidate a user's session even after the user initiated logout. It makes it possible for an attacker to reuse the admin cookies either via local/network access or by other hypothetical attacks.
	<b>CRITICAL</b> Vector: <b>network</b> Created: 2022-02-10 Updated: 2022-02-10

Source: NIST

NIST CVE: High

CVE-2021-45268	** DISPUTED ** A Cross Site Request Forgery (CSRF) vulnerability exists in <b>Backdrop</b> CMS 1.20, which allows Remote Attackers to gain Remote Code Execution (RCE) on the <b>Hosting</b> Webserver via uploading a maliciously add-on with crafted PHP file. NOTE: the vendor disputes this because the attack requires a session <b>cookie</b> of a high-privileged authenticated user who is entitled to install arbitrary add-ons.
	<b>HIGH</b> Vector: <b>network</b> Created: 2022-02-03 Updated: 2022-02-10

CVE-2022-22723	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted. Affected Product: Easergy P5 (All firmware versions prior to V01.401.101)
	<b>HIGH</b> Vector: <b>adjacent_network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2020-7534	A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists on the web server used, that could cause a leak of sensitive data or unauthorized actions on the web server during the time the user is logged in. Affected Products: <b>Modicon M340</b> CPUs: BMXP34 (All Versions), <b>Modicon Quantum</b> CPUs with integrated Ethernet (Copro): 140CPU65 (All Versions), Modicon Premium CPUs with integrated Ethernet (Copro): TSXP57 (All Versions), Modicon M340 ethernet modules: (BMXNOC0401, BMXNOE01, BMXNOR0200H) (All Versions), Modicon Quantum and Premium factory cast communication modules: (140NOE77111, 140NOC78*00, TSXETY5103, TSXETY4103) (All Versions)
	<b>HIGH</b> Vector: <b>network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2022-22150	A memory corruption vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 11.1.0.52543. A specially-crafted PDF document can trigger an exception which is improperly handled, leaving the engine in an invalid state, which can lead to memory corruption and arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.
	<b>HIGH</b> Vector: <b>network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2021-42113	An issue was discovered in StorageSecurityCommandDxe in <b>Insyde</b> InsydeH2O with Kernel 5.1 before 05.14.28, Kernel 5.2 before 05.24.28, and Kernel 5.3 before 05.32.25. An SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.
	<b>HIGH</b> Vector: <b>local</b> Created: 2022-02-03 Updated: 2022-02-10

CVE-2022-22689	CA Harvest Software Change Manager versions 13.0.3, 13.0.4, 14.0.0, and 14.0.1, contain a vulnerability in the CSV export functionality, due to insufficient input validation, that can allow a privileged user to potentially execute arbitrary code or commands.
	<b>HIGH</b> Vector: <b>network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2022-23590	<b>Tensorflow</b> is an Open Source Machine Learning Framework. A `GraphDef` from a TensorFlow `SavedModel` can be maliciously altered to cause a TensorFlow process to crash due to encountering a `StatusOr` value that is an error and forcibly extracting the value from it. We have patched the issue in multiple <b>GitHub</b> commits and these will be included in TensorFlow 2.8.0 and TensorFlow 2.7.1, as both are affected.
	<b>HIGH</b> Vector: <b>network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2022-23591	<b>Tensorflow</b> is an Open Source Machine Learning Framework. The `GraphDef` format in TensorFlow does not allow self recursive functions. The <b>runtime</b> assumes that this invariant is satisfied. However, a `GraphDef` containing a fragment such as the following can be consumed when loading a `SavedModel`. This would result in a stack overflow during execution as resolving each `NodeDef` means resolving the function itself and its nodes. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.
	<b>HIGH</b> Vector: <b>network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2022-22725	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted. Affected Product: Easergy P3 (All versions prior to V30.205)
	<b>HIGH</b> Vector: <b>adjacent_network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2022-22727	A CWE-20: Improper Input Validation vulnerability exists that could allow an unauthenticated attacker to view data, change settings, impact availability of the software, or potentially impact a user's local machine when the user clicks a specially crafted link. Affected Product: <b>EcoStruxure Power Monitoring Expert</b> (Versions 2020 and prior)
	<b>HIGH</b> Vector: <b>network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2022-22722	A CWE-798: Use of Hard-coded Credentials vulnerability exists that could result in information disclosure. If an attacker were to obtain the SSH cryptographic key for the device and take active control of the local operational network connected to the product they could potentially observe and manipulate traffic associated with product configuration. Affected Product: Easergy P5 (All firmware versions prior to V01.401.101)
	<b>HIGH</b> Vector: <b>adjacent_network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2021-4154	A use-after-free flaw was found in cgroup1_parse_param in kernel/cgroup/cgroup-v1.c in the <b>Linux</b> kernel's cgroup v1 parser. A local attacker with a user privilege could cause a privilege escalation by exploiting the fsconfig syscall parameter leading to a container breakout and a denial of service on the system.
	<b>HIGH</b> Vector: <b>local</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2021-43323	An issue was discovered in UsbCoreDxe in <b>Insyde</b> InsydeH2O with kernel 5.5 before 05.51.45, 5.4 before 05.43.45, 5.3 before 05.35.45, 5.2 before 05.26.45, 5.1 before 05.16.45, and 5.0 before 05.08.45. An SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.
	<b>HIGH</b> Vector: <b>local</b> Created: 2022-02-03 Updated: 2022-02-10

CVE-2022-0481	NULL Pointer Dereference in Homebrew <b>mruby</b> prior to 3.2.
	<b>HIGH</b> Vector: <b>network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2022-23592	<b>Tensorflow</b> is an Open Source Machine Learning Framework. TensorFlow's type inference can cause a heap out of bounds read as the bounds checking is done in a `DCHECK` (which is a no-op during production). An attacker can control the `input_idx` variable such that `ix` would be larger than the number of values in `node.targs`. The fix will be included in TensorFlow 2.8.0. This is the only affected version.
	<b>HIGH</b> Vector: <b>network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2022-23593	<b>Tensorflow</b> is an Open Source Machine Learning Framework. The `simplifyBroadcast` function in the MLIR-TFRT infrastructure in TensorFlow is vulnerable to a segfault (hence, denial of service), if called with scalar shapes. If all shapes are scalar, then `maxRank` is 0, so we build an empty `SmallVector`. The fix will be included in TensorFlow 2.8.0. This is the only affected version.
	<b>HIGH</b> Vector: <b>network</b> Created: 2022-02-04 Updated: 2022-02-10

CVE-2020-12965	When combined with specific software sequences, AMD CPUs may transiently execute non-canonical loads and store using only the lower 48 address bits potentially resulting in data leakage.
HIGH	Vector: network Created: 2022-02-04 Updated: 2022-02-10

Source: NIST

NIST CVE: Medium

CVE-2022-22726	A CWE-20: Improper Input Validation vulnerability exists that could allow arbitrary files on the server to be read by authenticated users through a limited operating system service account. Affected Product: <b>EcoStruxure Power Monitoring Expert</b> (Versions 2020 and prior)	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2022-0227	Business Logic Errors in <b>GitHub</b> repository silverstripe/silverstripe-framework prior to 4.10.1.	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2022-23581	<b>Tensorflow</b> is an Open Source Machine Learning Framework. The Grappler optimizer in TensorFlow can be used to cause a denial of service by altering a `SavedModel` such that `IsSimplifiableReshape` would trigger `CHECK` failures. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2022-23595	<b>Tensorflow</b> is an Open Source Machine Learning Framework. When building an XLA compilation cache, if default settings are used, TensorFlow triggers a null pointer dereference. In the default scenario, all devices are allowed, so `flr->config_proto` is `nullptr`. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2022-0380	The Fotobook <b>WordPress</b> plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient escaping and the use of <code>\$ SERVER['PHP_SELF']</code> found in the <code>~/options-fotobook.php</code> file which allows attackers to inject arbitrary web scripts onto the page, in versions up to and including 3.2.3.	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2022-22939	<b>VMware Cloud Foundation</b> contains an information disclosure vulnerability due to logging of credentials in plain-text within multiple log files on the SDDC Manager. A malicious actor with root access on VMware Cloud Foundation SDDC Manager may be able to view credentials in plaintext within one or more log files.	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2022-22804	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could allow an authenticated attacker to view data, change settings, or impact availability of the software when the user visits a page containing the injected payload. Affected Product: <b>EcoStruxure Power Monitoring Expert</b> (Versions 2020 and prior)	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2022-23580	<b>Tensorflow</b> is an Open Source Machine Learning Framework. During shape inference, TensorFlow can allocate a large vector based on a value from a tensor controlled by the user. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2022-23579	<b>Tensorflow</b> is an Open Source Machine Learning Framework. The Grappler optimizer in TensorFlow can be used to cause a denial of service by altering a `SavedModel` such that `SafeToRemoveIdentity` would trigger `CHECK` failures. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2022-0381	The Embed <b>Swagger WordPress</b> plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient escaping/sanitization and validation via the url parameter found in the <code>~/swagger-iframe.php</code> file which allows attackers to inject arbitrary web scripts onto the page, in versions up to and including 1.0.0.	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2022-0472	Unrestricted Upload of File with Dangerous Type in Packagist jsdecena/laracom prior to v2.0.9.	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10
CVE-2021-43841	<b>XWiki</b> is a generic wiki platform offering <b>runtime</b> services for applications built on top of it. When using default XWiki configuration, it's possible for an attacker to upload an <b>SVG</b> containing a script executed when executing the download <b>action</b> on the file. This problem has been patched so that the default configuration doesn't allow to display the SVG files in the browser. Users are advised to update or to disallow uploads of SVG files.	MEDIUM	Vector: network Created: 2022-02-04 Updated: 2022-02-10

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2021-22954	A cross-site request forgery vulnerability exists in <b>Concrete CMS</b>	UNRATED	Vector: unkown Created: 2022-02-09 Updated: 2022-02-10
CVE-2022-24313	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could cause a stack-based buffer overflow potentially leading to remote code execution when an attacker sends a specially crafted message. Affected Product: <b>Interactive Graphical SCADA System</b> Data Server (V15.0.0.22020 and prior)	UNRATED	Vector: unkown Created: 2022-02-09 Updated: 2022-02-10
CVE-2022-24314	A CWE-125: Out-of-bounds Read vulnerability exists that could cause memory leaks potentially resulting in denial of service when an attacker repeatedly sends a specially crafted message. Affected Product: <b>Interactive Graphical SCADA System</b> Data Server (V15.0.0.22020		
CVE-2022-22807	A CWE-1021 Improper Restriction of Rendered UI Layers or Frames vulnerability exists that could cause unintended modifications of the product settings or user accounts when deceiving the user to use the <b>web interface</b> rendered within iframes. Affected Product: EcoStruxure EV Charging Expert (formerly known as EVlink Load Management System): (HMIBSCEA53D1EDB, HMIBSCEA53D1EDS, HMIBSCEA53D1EDM, HMIBSCEA53D1EDL, HMIBSCEA53D1ESS, HMIBSCEA53D1ESM, HMIBSCEA53D1EML) (All Versions prior to SP8 (Version 01) V4.0.0.13)	UNRATED	Vector: unkown Created: 2022-02-09 Updated: 2022-02-10
CVE-2022-24315	A CWE-125: Out-of-bounds Read vulnerability exists that could cause denial of service when an attacker repeatedly sends a specially crafted message. Affected Product: <b>Interactive Graphical SCADA System</b> Data Server (V15.0.0.22020 and prior)	UNRATED	Vector: unkown Created: 2022-02-09 Updated: 2022-02-10
CVE-2022-24310	A CWE-190: Integer Overflow or Wraparound vulnerability exists that could cause heap-based buffer overflow, leading to denial of service and potentially remote code execution when an attacker sends multiple specially crafted messages. Affected Product: <b>Interactive Graphical</b>		



	<div>and prior)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-24312	<div>A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists that could cause modification of an existing file by adding at end of file or create a new file in the context of the Data Server potentially leading to remote code execution when an attacker sends a specially crafted message. Affected Product: <b>Interactive Graphical SCADA System</b> Data Server (V15.0.0.22020 and prior)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-22817	<div>A CWE-276: Incorrect Default Permissions vulnerability exists that could cause unauthorized access to the base installation directory leading to local privilege escalation. Affected Product: Harmony/Magelis iPC Series (All Versions), Vijeo <b>Designer</b> (All Versions prior to V6.2 SP11 Multiple HotFix 4), <b>Vijeo Designer</b> Basic (All Versions prior to V1.2.1)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-24319	<div>A CWE-295: Improper Certificate Validation vulnerability exists that could allow a Man-in-theMiddle attack when communications between the client and Geo <b>SCADA</b> web server are intercepted. Affected Product: <b>ClearSCADA</b> (All Versions), <b>EcoStruxure Geo SCADA Expert 2019</b> (All Versions), <b>EcoStruxure Geo SCADA Expert 2020</b> (All Versions)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-22810	<div>A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow an attacker to manipulate the admin after numerous attempts at guessing credentials. Affected Product: <b>spaceLYnk</b> (V2.6.2 and prior), Wiser for KNX (formerly homeLYnk) (V2.6.2 and prior), fellerLYnk (V2.6.2 and prior)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-22811	<div>A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists that could induce users to perform unintended actions, leading to the override of the system?s configurations when an attacker persuades a user to visit a rogue website. Affected Product: <b>spaceLYnk</b> (V2.6.2 and prior), Wiser for KNX (formerly homeLYnk) (V2.6.2 and prior), fellerLYnk (V2.6.2 and prior)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-24321	<div>A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause Denial of Service against the Geo <b>SCADA</b> server when receiving a malformed HTTP request. Affected Product: <b>ClearSCADA</b> (All Versions), <b>EcoStruxure Geo SCADA Expert 2019</b> (All Versions), <b>EcoStruxure Geo SCADA Expert 2020</b> (All Versions)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-22813	<div>A CWE-798: Use of Hard-coded Credentials vulnerability exists. If an attacker were to obtain the TLS cryptographic key and take active control of the Courier tunneling communication network, they could potentially observe and manipulate traffic associated with product configuration.</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-22808	<div>A CWE-942: Permissive Cross-domain Policy with Untrusted Domains vulnerability exists that could cause a remote attacker to gain unauthorized access to the product when conducting cross-domain attacks based on same-origin policy or cross-site request forgery protections bypass. Affected Product: EcoStruxure EV Charging Expert (formerly known as EVlink Load Management System): (HMIBSCEA53D1EDB, HMIBSCEA53D1EDS, HMIBSCEA53D1EDM, HMIBSCEA53D1EDL, HMIBSCEA53D1ESS, HMIBSCEA53D1ESM, HMIBSCEA53D1EML) (All Versions prior to SP8 (Version 01) V4.0.0.13)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-0530	<div>A flaw was found in <b>unzip</b> 6.0. The vulnerability occurs during the conversion of an utf-8 string to a local string that leads to a segmentation fault. This flaw allows an attacker to input a specially crafted zip file, leading to a crash or code execution.</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-22545	<div>A high privileged user who has access to transaction SM59 can read connection details stored with the destination for http calls in SAP <b>NetWeaver Application Server</b> ABAP and ABAP Platform - versions 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756.</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>

	<div><b>SCADA System</b> Data Server (V15.0.0.22020 and prior)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-24311	<div>A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists that could cause modification of an existing file by inserting at beginning of file or create a new file in the context of the Data Server potentially leading to remote code execution when an attacker sends a specially crafted message. Affected Product: <b>Interactive Graphical SCADA System</b> Data Server (V15.0.0.22020 and prior)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-24320	<div>A CWE-295: Improper Certificate Validation vulnerability exists that could allow a Man-in-theMiddle attack when communications between the client and Geo <b>SCADA database server</b> are intercepted. Affected Product: <b>ClearSCADA</b> (All Versions), <b>EcoStruxure Geo SCADA Expert 2019</b> (All Versions), <b>EcoStruxure Geo SCADA Expert 2020</b> (All Versions)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-22809	<div>A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow modifications of the touch configurations in an unauthorized manner when an attacker attempts to modify the touch configurations. Affected Product: <b>spaceLYnk</b> (V2.6.2 and prior), Wiser for KNX (formerly homeLYnk) (V2.6.2 and prior), fellerLYnk (V2.6.2 and prior)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-24318	<div>A CWE-326: Inadequate Encryption Strength vulnerability exists that could cause non-encrypted communication with the server when outdated versions of the ViewX client are used. Affected Product: <b>ClearSCADA</b> (All Versions), <b>EcoStruxure Geo SCADA Expert 2019</b> (All Versions), <b>EcoStruxure Geo SCADA Expert 2020</b> (All Versions)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-24316	<div>A CWE-665: Improper Initialization vulnerability exists that could cause information exposure when an attacker sends a specially crafted message. Affected Product: <b>Interactive Graphical SCADA System</b> Data Server (V15.0.0.22020 and prior)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-22812	<div>A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a web session compromise when an attacker injects and then executes arbitrary malicious JavaScript code inside the target browser. Affected Product: <b>spaceLYnk</b> (V2.6.2 and prior), Wiser for KNX (formerly homeLYnk) (V2.6.2 and prior), fellerLYnk (V2.6.2 and prior)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-24317	<div>A CWE-862: Missing Authorization vulnerability exists that could cause information exposure when an attacker sends a specific message. Affected Product: <b>Interactive Graphical SCADA System</b> Data Server (V15.0.0.22020 and prior)</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-0391	<div>A flaw was found in Python, specifically within the urllib.parse module. This module helps break Uniform Resource <b>Locator</b> (URL) strings into components. The issue involves how the urlparse method does not sanitize input and allows characters like 'r' and 'n' in the URL path. This flaw allows an attacker to input a crafted URL, leading to injection attacks. This flaw affects Python versions prior to 3.10.0b1, 3.9.5, 3.8.11, 3.7.11 and 3.6.14.</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-0529	<div>A flaw was found in <b>unzip</b> 6.0. The vulnerability occurs during the conversion of <b>wide</b> string to local string that leads to a heap of out-of-bound writes. This flaw allows an attacker to input a specially crafted zip file, leading to a crash or code execution.</div> <div>UNRATEDVector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-24668	<div>A program using swift-nio-http2 is vulnerable to a denial of service attack caused by a network peer sending ALTSVC or <b>ORIGIN</b> frames. This attack affects all swift-nio-http2 versions from 1.0.0 to 1.19.1. This vulnerability is caused by a logical error after frame parsing but before frame handling. ORIGIN and ALTSVC frames are not currently supported by swift-nio-http2, and should be ignored. However, one code path that encounters them has a deliberate trap instead. This was left behind from the original development process and was never removed. Sending an ALTSVC or ORIGIN frame does not require any special permission, so any HTTP/2 connection peer may send such a frame. For clients, this means any server to which they connect may launch this attack. For servers, anyone they allow to connect to them may launch such an attack. The attack is low-effort: it takes very little <b>resources</b> to send one of these frames. The impact on availability is high: receiving the frame immediately crashes the server, dropping all in-flight connections and causing the service to need to restart. It is straightforward for an attacker to repeatedly send these frames, so attackers require very few resources to achieve a substantial denial of service. The attack does not have any confidentiality or integrity risks in and of itself. This is a controlled, intentional crash. However, sudden process crashes can lead to violations of invariants in services, so it is possible that this attack can be used to trigger an error condition that has confidentiality or integrity risks. The risk can be mitigated if</div>

CVE-2022-24667	<p>A program using swift-nio-http2 is vulnerable to a denial of service attack, caused by a network peer sending a specially crafted HPACK-encoded header block. This attack affects all swift-nio-http2 versions from 1.0.0 to 1.19.1. There are a number of implementation errors in the parsing of HPACK-encoded header blocks that allow maliciously crafted HPACK header blocks to cause crashes in processes using swift-nio-http2. Each of these crashes is triggered instead of an integer overflow. A malicious HPACK header block could be sent on any of the HPACK-carrying frames in a HTTP/2 connection (HEADERS and PUSH_PROMISE), at any position. Sending a HPACK header block does not require any special permission, so any HTTP/2 connection peer may send one. For clients, this means any server to which they connect may launch this attack. For servers, anyone they allow to connect to them may launch such an attack. The attack is low-effort: it takes very little <b>resources</b> to send an appropriately crafted field block. The impact on availability is high: receiving a frame carrying this field block immediately crashes the server, dropping all in-flight connections and causing the service to need to restart. It is straightforward for an attacker to repeatedly send appropriately crafted field blocks, so attackers require very few resources to achieve a substantial denial of service. The attack does not have any confidentiality or integrity risks in and of itself: swift-nio-http2 is parsing the field block in memory-safe code and the crash is triggered instead of an integer overflow. However, sudden process crashes can lead to violations of invariants in services, so it is possible that this attack can be used to trigger an error condition that has confidentiality or integrity risks. The risk can be mitigated if untrusted peers can be prevented from communicating with the service. This mitigation is not available to many services. The issue is fixed by rewriting the parsing code to correctly handle all conditions in the function. The principal issue was found by automated fuzzing by oss-fuzz, but several associated <b>bugs</b> in the same code were found by code audit and fixed at the same time</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	---

CVE-2022-0534	<p>A vulnerability was found in <b>htmldoc</b> version 1.9.15 where the stack out-of-bounds read takes place in gif_get_code() and occurs when opening a malicious GIF file, which can result in a crash (segmentation fault).</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
---------------	---

CVE-2021-36302	<p>All <b>Dell</b> EMC Integrated System for <b>Microsoft Azure</b> Stack Hub versions contain a privilege escalation vulnerability. A remote malicious user with standard level JEA credentials may potentially exploit this vulnerability to elevate privileges and take over the system.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2021-41442	<p>An HTTP smuggling attack in the web application of <b>D-Link</b> DIR-X1860 before v1.10WWB09 Beta allows a remote unauthenticated attacker to DoS the web application via sending a specific HTTP packet.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	---

CVE-2022-0532	<p>An incorrect sysctls validation vulnerability was found in <b>CRI-O</b> 1.18 and earlier. The sysctls from the list of "safe" sysctls specified for the cluster will be applied to the host if an attacker is able to create a pod with a hostIPC and hostNetwork kernel namespace.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
---------------	---

CVE-2021-0115	<p>Buffer overflow in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
---------------	--

CVE-2021-45286	<p>Directory Traversal vulnerability exists in <b>ZZCMS</b> 2021 via the skin parameter in 1) index.php, 2) bottom.php, and 3) top_index.php.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-22546	<p>Due to improper HTML encoding in input control summary, an authorized attacker can execute XSS vulnerability in SAP Business Objects <b>Web Intelligence</b> (BI Launchpad) - version 420.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-23047	<p><b>Exponent CMS</b> 2.6.0patch2 allows an authenticated admin user to inject persistent JavaScript code inside the "Site/Organization Name","Site Title" and "Site Header" parameters while updating the site settings on "/exponentcms/administration/configure_site"</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-23049	<p><b>Exponent CMS</b> 2.6.0patch2 allows an authenticated user to inject persistent JavaScript code on the "User-Agent" header when logging in. When an administrator user visits the "User Sessions" tab, the JavaScript will be triggered allowing an attacker to compromise the administrator session.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	---

untrusted peers can be prevented from communicating with the service. This mitigation is not available to many services. The issue is fixed by rewriting the parsing code to correctly handle the condition. The issue was found by automated fuzzing by oss-fuzz.
UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10

CVE-2022-24666	<p>A program using swift-nio-http2 is vulnerable to a denial of service attack, caused by a network peer sending a specially crafted HTTP/2 <b>frame</b>. This attack affects all swift-nio-http2 versions from 1.0.0 to 1.19.1. This vulnerability is caused by a logical error when parsing a HTTP/2 HEADERS frame where the frame contains priority information without any other data. This logical error caused confusion about the size of the frame, leading to a parsing error. This parsing error immediately crashes the entire process. Sending a HEADERS frame with HTTP/2 priority information does not require any special permission, so any HTTP/2 connection peer may send such a frame. For clients, this means any server to which they connect may launch this attack. For servers, anyone they allow to connect to them may launch such an attack. The attack is low-effort: it takes very little <b>resources</b> to send an appropriately crafted frame. The impact on availability is high: receiving the frame immediately crashes the server, dropping all in-flight connections and causing the service to need to restart. It is straightforward for an attacker to repeatedly send appropriately crafted frames, so attackers require very few resources to achieve a substantial denial of service. The attack does not have any confidentiality or integrity risks in and of itself: swift-nio-http2 is parsing the frame in memory-safe code, so the crash is safe. However, sudden process crashes can lead to violations of invariants in services, so it is possible that this attack can be used to trigger an error condition that has confidentiality or integrity risks. The risk can be mitigated if untrusted peers can be prevented from communicating with the service. This mitigation is not available to many services. The issue is fixed by rewriting the parsing code to correctly handle the condition. The issue was found by automated fuzzing by oss-fuzz.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-21156	<p>Access of uninitialized pointer in the Intel(R) Trace <b>Analyzer</b> and <b>Collector</b> before version 2021.5 may allow an authenticated user to potentially enable denial of service via local access.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2021-39943	<p>An authorization logic error in the External <b>Status</b> Check API in <b>GitLab</b> EE affecting all versions starting from 14.1 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allowed a user to update the status of the check via an API call</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-21825	<p>An Improper Access Control vulnerability exists in <b>Citrix Workspace</b> App for <b>Linux</b> 2012 - 2111 with App Protection installed that can allow an attacker to perform local privilege escalation.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	---

CVE-2021-26616	<p>An OS command injection was found in SecuwaySSL, when special characters injection on execute command with runCommand arguments.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-0558	<p>Cross-site Scripting (XSS) - Stored in Packagist microweber/microweber prior to 1.2.11.</p> <div>UNRATED Vector: unknown Created: 2022-02-10 Updated: 2022-02-10</div>
---------------	---

CVE-2022-22533	<p>Due to improper error handling in SAP <b>NetWeaver Application Server Java</b> - versions KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, an attacker could submit multiple HTTP server requests resulting in errors, such that it consumes the memory buffer. This could result in system shutdown rendering the system unavailable.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-22534	<p>Due to insufficient encoding of user input, SAP <b>NetWeaver</b> allows an unauthenticated attacker to inject code that may expose sensitive data like <b>user ID</b> and password. These endpoints are normally exposed over the network and successful exploitation can partially impact confidentiality of the application.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-23048	<p><b>Exponent CMS</b> 2.6.0patch2 allows an authenticated admin user to upload a malicious extension in the format of a ZIP file with a PHP file inside it. After upload it, the PHP file will be placed at "themes/simpletheme/{rce}.php" from where can be accessed in order to execute commands.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	---

CVE-2021-0166	<p>Exposure of Sensitive Information to an Unauthorized Actor in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow a privileged user to potentially enable escalation of privilege via local access.</p> <div>UNRATED Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</div>
---------------	--

CVE-2021-0170	<p>Exposure of Sensitive Information to an Unauthorized Actor in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an authenticated user to potentially enable information disclosure via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2022-21174	<p>Improper access control in a third-party component of Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0167	<p>Improper access control in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow a privileged user to potentially enable escalation of privilege via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0092	<p>Improper access control in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable a denial of service via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0091	<p>Improper access control in the firmware for some Intel(R) Processors may allow an unauthenticated user to potentially enable an escalation of privilege via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2022-21153	<p>Improper access control in the Intel(R) Capital Global <b>Summit Android</b> application may allow an authenticated user to potentially enable information disclosure via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2022-21157	<p>Improper access control in the Intel(R) Smart Campus <b>Android</b> application before version 6.1 may allow authenticated user to potentially enable information disclosure via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-33147	<p>Improper conditions check in the Intel(R) IPP <b>Crypto</b> library before version 2021.2 may allow an authenticated user to potentially enable information disclosure via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0125	<p>Improper initialization in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via physical access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-33114	<p>Improper input validation for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and Killer(TM) WiFi in <b>Windows</b> 10 and 11 may allow an authenticated user to potentially enable denial of service via adjacent access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-33115	<p>Improper input validation for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-44454	<p>Improper input validation in a third-party component for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0165	<p>Improper input validation in firmware for Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0176	<p>Improper input validation in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow a privileged user to potentially enable denial of service via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0072	<p>Improper input validation in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow a privileged user to potentially enable information disclosure via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-33155	<p>Improper input validation in firmware for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products before version</p>

CVE-2022-21660	<p>Gin-vue-admin is a <b>backstage</b> management system based on vue and gin. In versions prior to 2.4.7 low privilege users are able to modify higher privilege users. Authentication is missing on the `setUserInfo` function. Users are advised to update as soon as possible. There are no known workarounds.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0164	<p>Improper access control in firmware for Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable escalation of privilege via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0171	<p>Improper access control in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an authenticated user to potentially enable information disclosure via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0124	<p>Improper access control in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via physical access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-23152	<p>Improper access control in the Intel(R) <b>Advisor</b> software before version 2021.2 may allow an authenticated user to potentially enable escalation of privilege via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-33119	<p>Improper access control in the Intel(R) RealSense(TM) DCM before version 20210625 may allow an authenticated user to potentially enable information disclosure via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-33139	<p>Improper conditions check in firmware for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products before version 22.100 may allow an authenticated user to potentially enable denial of service via adjacent access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0119	<p>Improper initialization in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via physical access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0145	<p>Improper initialization of shared <b>resources</b> in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-33113	<p>Improper input validation for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and Killer(TM) WiFi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-33110	<p>Improper input validation for some Intel(R) Wireless Bluetooth(R) products and Killer(TM) Bluetooth(R) products in <b>Windows</b> 10 and 11 before version 22.80 may allow an unauthenticated user to potentially enable denial of service via adjacent access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0161	<p>Improper input validation in firmware for Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow a privileged user to potentially enable escalation of privilege via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0066	<p>Improper input validation in firmware for Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable escalation of privilege via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0168	<p>Improper input validation in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow a privileged user to potentially enable escalation of privilege via local access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0172	<p>Improper input validation in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.</p> <p><b>UNRATED</b> Vector: unknown Created: 2022-02-09 Updated: 2022-02-10</p>
CVE-2021-0178	<p>Improper input validation in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an</p>

	<div>22.100 may allow an authenticated user to potentially enable denial of service via adjacent access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>unauthenticated user to potentially enable denial of service via adjacent access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2021-0162	<div>Improper input validation in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2021-0156</div> <div>Improper input validation in the firmware for some Intel(R) Processors may allow an authenticated user to potentially enable an escalation of privilege via local access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2021-26613	<div>improper input validation vulnerability in <b>nexacro</b> permits copying file to the startup folder using <b>rename</b> method.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2021-33096</div> <div>Improper isolation of shared <b>resources</b> in network on chip for the Intel(R) 82599 Ethernet Controllers and Adapters may allow an authenticated user to potentially enable denial of service via local access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2021-0147	<div>Improper locking in the <b>Power Management</b> Controller (PMC) for some <b>Intel</b> Chipset firmware before versions pmc_fw_lbg_c1-21ww02a and pmc_fw_lbg_b0-21ww02a may allow a privileged user to potentially enable denial of service via local access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2022-21204</div> <div>Improper permissions for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2022-21203	<div>Improper permissions in the SafeNet <b>Sentinel</b> driver for Intel(R) Quartus(R) Prime Standard Edition before version 21.1 may allow an authenticated user to potentially enable escalation of privilege via local access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2022-21220</div> <div>Improper restriction of XML external entity for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2022-21205	<div>Improper restriction of XML external entity reference in DSP Builder Pro for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an unauthenticated user to potentially enable information disclosure via network access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2021-0174</div> <div>Improper Use of Validation Framework in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow a unauthenticated user to potentially enable denial of service via adjacent access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2021-0179	<div>Improper Use of Validation Framework in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2021-0173</div> <div>Improper Validation of Consistency within input in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow a unauthenticated user to potentially enable denial of service via adjacent access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2021-0177	<div>Improper Validation of Consistency within input in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2021-0163</div> <div>Improper Validation of Consistency within input in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2021-0076	<div>Improper Validation of Specified Index, Position, or Offset in Input in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow a privileged user to potentially enable denial of service via local access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2021-0175</div> <div>Improper Validation of Specified Index, Position, or Offset in Input in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2021-0183	<div>Improper Validation of Specified Index, Position, or Offset in Input in software for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in <b>Windows</b> 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2022-20041</div> <div>In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108596; Issue ID: ALPS06108596.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2022-20043	<div>In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06148177; Issue ID: ALPS06148177.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2022-20042</div> <div>In Bluetooth, there is a possible information disclosure due to incorrect error handling. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108487; Issue ID: ALPS06108487.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2022-20046	<div>In Bluetooth, there is a possible memory corruption due to a logic error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06142410; Issue ID: ALPS06142410.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2022-20027</div> <div>In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126826; Issue ID: ALPS06126826.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2022-20026	<div>In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126827; Issue ID: ALPS06126827.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2022-20025</div> <div>In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126832; Issue ID: ALPS06126832.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2022-20028	<div>In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198663; Issue ID: ALPS06198663.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>	<div>CVE-2022-20044</div> <div>In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126814; Issue ID: ALPS06126814.</div> <div>UNRATEDVector: unknownCreated: 2022-02-09Updated: 2022-02-10</div>
CVE-2022-20045	<div>In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126820; Issue ID: ALPS06126820.</div>	<div>CVE-2022-20033</div> <div>In camera driver, there is a possible out of bounds read 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: ALPS05862973; Issue ID: ALPS05862973.</div>



	<div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20038	<div>In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183335; Issue ID: ALPS06183335.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20029	<div>In cmdq driver, there is a possible out of bounds read 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: ALPS05747150; Issue ID: ALPS05747150.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20017	<div>In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862991; Issue ID: ALPS05862991.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20037	<div>In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171705; Issue ID: ALPS06171705.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20034	<div>In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. 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 not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20024	<div>In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20032	<div>In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-33166	<div>Incorrect default permissions for the Intel(R) RXT for <b>Chromebook</b> application, all versions, may allow an authenticated user to potentially enable information disclosure via local access.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-33129	<div>Incorrect default permissions in the software installer for the Intel(R) <b>Advisor</b> before version 2021.4.0 may allow an authenticated user to potentially enable escalation of privilege via local access.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-33061	<div>Insufficient control flow management for the Intel(R) 82599 Ethernet Controllers and Adapters may allow an authenticated user to potentially enable denial of service via local access.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-0103	<div>Insufficient control flow management in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-33107	<div>Insufficiently protected credentials in USB provisioning for Intel(R) AMT SDK before version 16.0.3, Intel(R) SCS before version 12.2 and Intel(R) MEBx before versions 11.0.0.0012, 12.0.0.0011, 14.0.0.0004 and 15.0.0.0004 may allow an unauthenticated user to potentially enable information disclosure via physical access.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-0111	<div>NULL pointer dereference in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.</div>

	<div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20039	<div>In ccu driver, there is a possible memory corruption 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: ALPS06183345; Issue ID: ALPS06183345.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20031	<div>In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20036	<div>In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171689; Issue ID: ALPS06171689.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20040	<div>In power_hal manager service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-22532	<div>In SAP <b>NetWeaver Application Server Java</b> - versions KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, an unauthenticated attacker could submit a crafted HTTP server request which triggers improper shared memory buffer handling. This could allow the malicious payload to be executed and hence execute functions that could be impersonating the victim or even steal the victim's logon session.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20035	<div>In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-20030	<div>In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-0093	<div>Incorrect default permissions in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable a denial of service via local access.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-0060	<div>Insufficient compartmentalization in HECI subsystem for the Intel(R) SPS before versions SPS_E5_04.01.04.516.0, SPS_E5_04.04.04.033.0, SPS_E5_04.04.03.281.0, SPS_E5_03.01.03.116.0, SPS_E3_05.01.04.309.0, SPS_02.04.00.101.0, SPS_SoC-A_05.00.03.114.0, SPS_SoC-X_04.00.04.326.0, SPS_SoC-X_03.00.03.117.0, IGN_E5_91.00.00.167.0, SPS_PHI_03.01.03.078.0 may allow an authenticated user to potentially enable escalation of privilege via physical access.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-0127	<div>Insufficient control flow management in some Intel(R) Processors may allow an authenticated user to potentially enable a denial of service via local access.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-0099	<div>Insufficient control flow management in the firmware for some Intel(R) Processors may allow an authenticated user to potentially enable an escalation of privilege via local access.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-33068	<div>Null pointer dereference in subsystem for Intel(R) AMT before versions 15.0.35 may allow an authenticated user to potentially enable denial of service via network access.</div> <div>UNRATED</div> <div>Vector: unknow Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-23628	<div>OPA is an open source, general-purpose policy engine. Under certain conditions, pretty-printing an abstract syntax tree (AST) that contains synthetic nodes could change the logic of some statements by reordering array literals. Example of policies impacted are those that parse and compare web paths. <b>**All of these** three</b> conditions have to be met to create an adverse effect: 1. An AST of Rego had to be <b>**created programmatically**</b> such that it ends up containing terms without a location (such as wildcard variables). 2. The AST had to be <b>**pretty-printed**</b> using the `github.com/open-policy-agent/opa/format` package. 3. The result of the pretty-printing had to be <b>**parsed and evaluated again**</b> via an OPA instance using the bundles, or the <b>Golang</b> packages. If any of these three conditions are not met, you are not</div>

	<div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>affected. Notably, all three would be true if using <b>**optimized bundles**</b>, i.e. bundles created with 'opa build -O=1' or higher. In that case, the optimizer would fulfil condition (1.), the result of that would be pretty-printed when writing the bundle to disk, fulfilling (2.). When the bundle was then used, we'd satisfy (3.). As a workaround users may disable optimization when creating bundles.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2021-33120	<div>Out of bounds read under complex microarchitectural condition in memory subsystem for some <b>Intel</b> Atom(R) Processors may allow authenticated user to potentially enable information disclosure or cause denial of service via network access.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2021-33105</div> <div>Out-of-bounds read in some Intel(R) Core(TM) processors with Radeon(TM) RX <b>Vega</b> M GL integrated graphics before version 21.10 may allow an authenticated user to potentially enable information disclosure via local access.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2021-0118	<div>Out-of-bounds read in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2022-21133</div> <div>Out-of-bounds read in the Intel(R) Trace <b>Analyzer</b> and <b>Collector</b> before version 2021.5 may allow an authenticated user to potentially enable denial of service via local access.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2022-21226	<div>Out-of-bounds read in the Intel(R) Trace <b>Analyzer</b> and <b>Collector</b> before version 2021.5 may allow an authenticated user to potentially enable information disclosure via local access.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2021-0116</div> <div>Out-of-bounds write in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2021-33137	<div>Out-of-bounds write in the Intel(R) Kernelflinger project may allow an authenticated user to potentially enable escalation of privilege via local access.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2021-0117</div> <div>Pointer issues in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2022-22542	<div>S/4HANA Supplier Factsheet exposes the private address and bank details of an Employee Business Partner with Supplier Role, AND <b>Enterprise Search</b> for Customer, Supplier and Business Partner objects exposes the private address fields of Employee Business Partners, to an actor that is not explicitly authorized to have access to that information, which could compromise Confidentiality.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2022-22528</div> <div>SAP Adaptive Server Enterprise (ASE) - version 16.0, installation makes an entry in the system PATH environment variable in <b>Windows</b> platform which, under certain conditions, allows a Standard User to execute malicious Windows binaries which may lead to privilege escalation on the local system. The issue is with the ASE installer and does not impact other ASE binaries.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2022-22535	<div>SAP <b>ERP HCM</b> Portugal - versions 600, 604, 608, does not perform necessary authorization checks for a <b>report</b> that reads the <b>payroll</b> data of employees in a certain area. Since the affected report only reads the payroll information, the attacker can neither modify any information nor cause availability impacts.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2022-22536</div> <div>SAP <b>NetWeaver Application Server</b> ABAP, SAP <b>NetWeaver Application Server</b> Java, ABAP Platform, SAP Content Server 7.53 and SAP Web <b>Dispatcher</b> are vulnerable for request smuggling and request concatenation. An unauthenticated attacker can prepend a victim's request with arbitrary data. This way, the attacker can execute functions impersonating the victim or poison intermediary Web caches. A successful attack could result in complete compromise of Confidentiality, Integrity and Availability of the system.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2022-22543	<div>SAP <b>NetWeaver Application Server</b> for ABAP (Kernel) and ABAP Platform (Kernel) - versions KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, does not sufficiently validate sapsport information, which could lead to a Denial-of-Service attack. This allows an unauthorized remote user to provoke a breakdown of the SAP Web <b>Dispatcher</b> or Kernel work process. The crashed process can be restarted immediately, other processes are not affected.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2022-22540</div> <div>SAP <b>NetWeaver AS ABAP</b> (Workplace Server) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, allows an attacker to execute crafted database queries, that could expose the backend database. Successful attacks could result in disclosure of a table of contents from the system, but no risk of modification possible.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2022-22567	<div>Select <b>Dell</b> Client Commercial and Consumer platforms are vulnerable to an insufficient verification of data authenticity vulnerability. An authenticated malicious user may exploit this vulnerability in order to install modified <b>BIOS</b> firmware.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2022-22566</div> <div>Select <b>Dell</b> Client Commercial and Consumer platforms contain a pre-boot direct memory access (DMA) vulnerability. An authenticated attacker with physical access to the system may potentially exploit this vulnerability in order to execute arbitrary code on the device.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2022-22544	<div><b>Solution Manager</b> (Diagnostics Root Cause Analysis Tools) - version 720, allows an administrator to execute code on all connected <b>Diagnostics Agents</b> and browse files on their systems. An attacker could thereby control the managed systems. It is considered that this is a missing segregation of duty for the SAP Solution Manager administrator. Impacts of unauthorized execution of commands can lead to sensitive information disclosure, loss of system integrity and denial of service.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2022-23631</div> <div>superjson is a program to allow JavaScript expressions to be serialized to a <b>superset</b> of JSON. In versions prior to 1.8.1 superjson allows input to run arbitrary code on any server using superjson input without prior authentication or knowledge. The only requirement is that the server implements at least <b>one endpoint</b> which uses superjson during request processing. This has been patched in superjson 1.8.1. Users are advised to update. There are no known workarounds for this issue.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2022-22779	<div>The <b>Keybase</b> Clients for <b>macOS</b> and <b>Windows</b> before version 5.9.0 fails to properly remove exploded messages initiated by a user. This can occur if the receiving user switches to a non-chat feature and places the host in a sleep state before the sending user explodes the messages. This could lead to disclosure of sensitive information which was meant to be deleted from a user's filesystem.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2022-0162</div> <div>The vulnerability exists in <b>TP-Link TL-WR841N</b> V11 3.16.9 Build 160325 Rel.62500n wireless router due to <b>transmission</b> of authentication information in cleartextbase64 format. Successful exploitation of this vulnerability could allow a remote attacker to intercept credentials and subsequently perform administrative operations on the affected device through web-based management interface.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2022-22780	<div>The <b>Zoom</b> Client for <b>Meetings</b> chat functionality was susceptible to Zip bombing attacks in the following product versions: <b>Android</b> before version 5.8.6, iOS before version 5.9.0, <b>Linux</b> before version 5.8.6, <b>macOS</b> before version 5.7.3, and <b>Windows</b> before version 5.6.3. This could lead to availability issues on the client host by exhausting system <b>resources</b>.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>	<div>CVE-2021-40044</div> <div>There is a permission verification vulnerability in the <b>Bluetooth</b> module.Successful exploitation of this vulnerability may cause unauthorized operations.</div> <div>UNRATED</div> <div>Vector: unknown   Created: 2022-02-09   Updated: 2022-02-10</div>
CVE-2021-40015	<div>There is a race condition vulnerability in the binder driver subsystem in the kernel.Successful exploitation of this vulnerability may affect kernel stability.</div>	<div>CVE-2021-37109</div> <div>There is a security protection bypass vulnerability with the modem.Successful exploitation of this vulnerability may cause memory protection failure.</div>

	<div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-40045	<div>There is a vulnerability of signature verification mechanism failure in system upgrade through recovery mode.Successful exploitation of this vulnerability may affect service confidentiality.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-39994	<div>There is an arbitrary address access vulnerability with the product line test code.Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-39992	<div>There is an improper security permission configuration vulnerability on ACPU.Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-39986	<div>There is an unauthorized rewriting vulnerability with the memory access management module on ACPU.Successful exploitation of this vulnerability may affect service confidentiality.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-21218	<div>Uncaught exception in the Intel(R) Trace <b>Analyzer</b> and <b>Collector</b> before version 2021.5 may allow an authenticated user to potentially enable information disclosure via local access.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>

CVE-2021-0169	<div>Uncontrolled Search Path Element in software for Intel(R) PROSet/Wireless Wi-Fi in <b>Windows</b> 10 and 11 may allow a privileged user to potentially enable escalation of privilege via local access.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-22538	<div>When a user opens a manipulated <b>Adobe Illustrator</b> file format (.ai, ai.x3d) received from untrusted sources in <b>SAP 3D Visual Enterprise Viewer</b> - version 9.0, the application crashes and becomes temporarily unavailable to the user until restart of the application. The file format details along with their CVE relevant information can be found below.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>

CVE-2022-22537	<div>When a user opens a manipulated Tagged Image File Format (.tiff, 2d.x3d)) received from untrusted sources in <b>SAP 3D Visual Enterprise Viewer</b> - version 9.0, the application crashes and becomes temporarily unavailable to the user until restart of the application. The file format details along with their CVE relevant information can be found below.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-23617	<div><b>XWiki</b> Platform is a generic wiki platform offering <b>runtime</b> services for applications built on top of it. In affected versions any user with edit right can copy the content of a page it does not have access to by using it as template of a new page. This issue has been patched in XWiki 13.2CR1 and 12.10.6. Users are advised to update. There are no known workarounds for this issue.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	---

CVE-2022-23615	<div><b>XWiki</b> Platform is a generic wiki platform offering <b>runtime</b> services for applications built on top of it. In affected versions any user with SCRIPT right can save a document with the right of the current user which allow accessing API requiring programming right if the current user has programming right. This has been patched in XWiki 13.0. Users are advised to update to resolve this issue. The only known workaround is to limit SCRIPT access.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	---

CVE-2022-23619	<div><b>XWiki</b> Platform is a generic wiki platform offering <b>runtime</b> services for applications built on top of it. In affected versions it's possible to guess if a user has an account on the wiki by using the "Forgot your password" form, even if the wiki is closed to guest users. This problem has been patched on XWiki 12.10.9, 13.4.1 and 13.6RC1. Users are advised yo update. There are no known workarounds for this issue.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

	<div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-39997	<div>There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-37107	<div>There is an improper memory access permission configuration on ACPU.Successful exploitation of this vulnerability may cause out-of-bounds access.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-37115	<div>There is an unauthorized rewriting vulnerability with the memory access management module on ACPU.Successful exploitation of this vulnerability may affect service confidentiality.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-39991	<div>There is an unauthorized rewriting vulnerability with the memory access management module on ACPU.Successful exploitation of this vulnerability may affect service confidentiality.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2021-0107	<div>Unchecked return value in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>

CVE-2021-33101	<div>Uncontrolled search path in the Intel(R) GPA software before version 21.2 may allow an authenticated user to potentially enable escalation of privilege via local access.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
CVE-2022-22539	<div>When a user opens a manipulated <b>JPEG</b> file format (.jpg, 2d.x3d) received from untrusted sources in <b>SAP 3D Visual Enterprise Viewer</b> - version 9.0, the application crashes and becomes temporarily unavailable to the user until restart of the application. The file format details along with their CVE relevant information can be found below.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>

CVE-2022-23620	<div><b>XWiki</b> Platform is a generic wiki platform offering <b>runtime</b> services for applications built on top of it. In affected versions AbstractSxExportURLFactoryActionHandler#processSx does not escape anything from SSX document references when serializing it on filesystem, it is possible to for the HTML export process to contain reference elements containing filesystem syntax like "../", "./.", or "/" in general. The referenced elements are not properly escaped. This issue has been resolved in version 13.6-rc-1. This issue can be worked around by limiting or disabling document export.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-23621	<div><b>XWiki</b> Platform is a generic wiki platform offering <b>runtime</b> services for applications built on top of it. In affected versions any user with SCRIPT right can read any file located in the XWiki WAR (for example xwiki.cfg and xwiki.properties) through XWiki#invokeServletAndReturnAsString as ` \$xwiki.invokeServletAndReturnAsString("/WEB-INF/xwiki.cfg")` . This issue has been patched in XWiki versions 12.10.9, 13.4.3 and 13.7-rc-1. Users are advised to update. The only workaround is to limit SCRIPT right.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-23616	<div><b>XWiki</b> Platform is a generic wiki platform offering <b>runtime</b> services for applications built on top of it. In affected versions it's possible for an unprivileged user to perform a remote code execution by injecting a <b>groovy</b> script in her own profile and by calling the <b>Reset password</b> feature since the feature is performing a save of the user profile with programming rights in the impacted versions of XWiki. The issue has been patched in XWiki 13.1RC1. There are two different possible workarounds, each consisting of modifying the XWiki/ResetPassword page. 1. The Reset password feature can be entirely disabled by deleting the XWiki/ResetPassword page. 2. The script in XWiki/ResetPassword can also be modified or removed: an administrator can replace it with a simple email contact to ask an administrator to reset the password.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	---

CVE-2022-23622	<div><b>XWiki</b> Platform is a generic wiki platform offering <b>runtime</b> services for applications built on top of it. In affected versions there is a cross site scripting (XSS) vector in the `registerinline.vm` template related to the `xredirect` hidden field. This template is only used in the following conditions: 1. The wiki must be open to registration for anyone. 2. The wiki must be closed to view for Guest users or more specifically the XWiki.Registration page must be forbidden in View for guest user. A way to obtain the second condition is when administrators checked the "Prevent unregistered users from viewing pages, regardless of the page rights" box in the administration rights. This issue is patched in versions 12.10.11, 14.0-rc-1, 13.4.7, 13.10.3. There are two main ways for protecting against this vulnerability, the easiest and the best one is by applying a patch in the `registerinline.vm` template, the patch consists in checking the value of the xredirect field to ensure it matches: ``. If for some reason it's not possible to patch this file, another workaround is to ensure "Prevent unregistered users from viewing pages, regardless of the page rights" is not checked in the rights and apply a better right scheme using groups and rights on <b>spaces</b>.</div> <div>UNRATED</div> <div>Vector: unkown Created: 2022-02-09 Updated: 2022-02-10</div>
----------------	--

CVE-2022-23618

XWiki Platform is a generic wiki platform offering **runtime** services for applications built on top of it. In affected versions there is no protection against URL **redirection** to untrusted sites, in particular some well known parameters (xredirect) can be used to perform url redirections. This problem has been patched in XWiki 12.10.7 and XWiki 13.3RC1. Users are advised to update. There are no known workarounds for this issue.

UNRATED

Vector: unkown

Created: 2022-02-09

Updated: 2022-02-10

Source: [Hybrid Analysis](#)

Top malicious files

100% Threat score	tmpi9awbic9	100% Threat score	Antitest (.) exe
100% Threat score	4dotsFreePDFCompressSetup (.) exe	100% Threat score	4dotsFreePDFCompress (.) exe
100% Threat score	NEW PO ORDER NO NO HS212839 (.) exe	100% Threat score	Outline-Manager (.) exe
100% Threat score	Patch (.) exe	100% Threat score	Justf2101 (.) exe
100% Threat score	auth (.) dll	100% Threat score	tmpsk20bxow
100% Threat score	document_word (.) pif	100% Threat score	reverse_shell_tp2 - Packer (.) exe
100% Threat score	wrapper (.) dll	100% Threat score	vbc (.) exe
100% Threat score	640a49413f5243c9c87afc7abdc2d51fcc2657b851b20634a250e6715790f0f (.) vbs	85% Threat score	Power-user (.) exe
85% Threat score	XD_Set-Up (.) exe	85% Threat score	Alon_setup_2022 (.) exe
77% Threat score	script (.) js	76% Threat score	oim (.) wcarina@seadrill (.) com_0416 (.) html
75% Threat score	paint (.) net (.) 4 (.) 3 (.) 7 (.) install (.) x64 (.) exe		

Source: [Hybrid Analysis](#)

Top malicious URL







100% Threat score	http://my (.) famous (.) co/jhq1z9w1mm/	100% Threat score	http://my (.) famous (.) co/4cxes55h5w/
100% Threat score	https://ams3 (.) digitaloceanspaces (.) com/awtydu2mbrkndgw1/14rfqg89o/br (.) dgw1 (.) html	91% Threat score	http://7rydlech (.) cn/
89% Threat score	http://7rydlech (.) cn/	87% Threat score	https://moodle (.) org/mod/forum/discuss (.) php?d=128731
83% Threat score	https://my (.) famous (.) co/	83% Threat score	http://my-k (.) ro/
80% Threat score	https://eroticcall (.) top/	77% Threat score	http://vanyog (.) com/index (.) php?pid=107
77% Threat score	http://vanyog (.) com/dr/contact	77% Threat score	http://instatourism (.) com/
74% Threat score	http://telugurajyam (.) com/	74% Threat score	https://trailer (.) web-view (.) net/Links/0XB5E87F70B6CE12DE70E8095A633A65028662A61FB2A0CC3FF6AF76D928BC296A497A879CF0540A43D7BDBC (.) htm
72% Threat score	http://vanyog (.) com/cyr-lat (.) php	72% Threat score	http://vanyog (.) com/_new/index (.) php?lid=390&pid=29#outer_links
72% Threat score	http://vanyog (.) com/typing/10finger (.) php	72% Threat score	http://my (.) famous (.) co/4cxes55h5w/
72% Threat score	http://vanyog (.) com/php/count (.) php?cyr-lat (.) exe	72% Threat score	http://voldoboosting24 (.) com/
72% Threat score	http://cansal (.) cl/ms/wamp (.) php?cramp=020202	72% Threat score	http://my (.) famous (.) co/mt6qwjsyt/*
72% Threat score	http://my (.) famous (.) co/jhq1z9w1mm/	72% Threat score	https://my (.) famous (.) co/pfh5s55565



		Threat score	
72% Threat score	<a href="http://my(.)famous(.)co/mt6qwjysyt/">http://my (.) famous (.) co/mt6qwjysyt/</a>		










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 Korea, Republic of








Source: [SpamHaus](#)

## Top spammers

 <b>#1 Canadian Pharmacy</b> 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.	 <b>#2 PredictLabs / Sphere Digital</b> 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.
 <b>#3 Hosting Response / Michael Boehm</b> 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.	 <b>#4 Mint Global Marketing / Adgenics / Cabo Networks</b> Florida affiliate spammers and bulletproof spam hosters
 <b>#5 RetroCubes</b> 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.	 <b>#6 Michael Persaud</b> Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.
 <b>#7 Cyber World Internet Services/ e-Insites</b> 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.	 <b>#8 RR Media</b> A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.
 <b>#9 Kobeni Solutions</b> 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 Indonesia
 #5 Thailand	 #6 Algeria
 #7 Viet Nam	 #8 Brazil
 #9 Iran (Islamic Republic of)	 #10 Pakistan

Source: [SpamHaus](#)

## Top phishing countries

 #1 United States	 #2 Netherlands
 #3 Germany	 #4 Russia
 #5 Hong Kong	 #6 France

	#7 Singapore		#8 United Kingdom
	#9 India		#10 Brazil