



Your Security Rabbits report for February 09, 2022

Hot topics

Feb 22 Patch Tuesday

This is Feb 2022 Microsoft Patch Tuesday.

The good news, nothing critical that requires emergency patching. There is a zero-day fix but there's no active exploit to this day.

All in all Microsoft fixed 48 vulnerabilities of which 16 are remote. If you a Windows DNS server with dynamic updates enabled, consider applying KB5010342 first.

--
JL Dupont

Twitter



Immanuel Chavoya

Not an Industrial Control System Router with a CRITICAL vulnerability allowing remote authenticated attackers the ability to inject/execute arbitrary shell commands as ROOT CVE-2022-0365 CVSS: 9.1 Default Admin Creds: Admin () #infosec #ics #ricon



ThreatMeter

CVE-2022-23329 A vulnerability in \${freemarker.template.utility.Execute?new()} of UJCMS Jspxcms v10.2.0 allows attackers to execute arbitrary commands via uploading malicious files. (CVSS:0.0) (Last Update:2022-02-04)



RedPacket Security

Ricon Mobile S9922XL and Ricon Mobile S9922L command execution | CVE-2022-0365 -



SRM IT Risk

IT Risk: HPE.ArubaOS-CX 8000 -2/3 CVE-2021-41839 CVE-2020-27339 CVE-2021-33626 CVE-2021-33627 CVE-2021-418 CVE-2021-418 CVE-2021-418 CVE-2021-41837 CVE-2021-43323 CVE-2021-42554 CVE-2021-33625 CVE-2021-43522 CVE-2021-42113 CVE-2021-42113



SRM IT Risk

IT Risk: Multiple Vulnerabilities in HPE.Aruba 9000 -2/2 CVE-2021-41610 CVE-2021-41840 CVE-2021-41839 CVE-2020-27339 CVE-2021-33626 CVE-2021-33627 CVE-2021-41838 CVE-2021-41837 CVE-2021-43323 CVE-2021-42554 CVE-2021-33625 CVE-2021-43522 CVE-2021-42113 CVE-2021-42059



Wolfgang Sesin

New post from (CVE-2021-23470 (putil-merge)) has been published on



Vulmon Vulnerability Feed

CVE-2021-36152 Apache Goblin trusts all certificates used for LDAP connections in Goblin-as-a-Service. This affects versions <= 0.15.0. Users should update to version 0.16.0 which addresses this issue.



Angenoire

#CyberSecurity #Security #CERT #CVE #Nist #breach #vulnerability : CVE-2021-23470



Remotely Alerts

Severity: | Unauthenticated SQL Injection (SQLi) vul... | CVE-2021-44779 | Link for more:



SRM IT Risk

IT Risk: HPE.Multiple Vulnerabilities in ArubaOS-CX 8000 Series Switches -2/3 CVE:CVE-2020-5953 CVE-2021-41610 CVE-2021-41840 CVE-2021-41841 CVE-2021-41839 CVE-2020-27339 CVE-2021-33626 CVE-2021-33627 CVE-2021-418 CVE-2021-418 CVE-2021-41837 CVE-2021-43323 CVE-2021-42554



3

CISA Vuln Summary - Week of 1.31.22 - Top CVSS: -insyde -- insydeh2o-CVE-2021-42554 (10) -totolink -- a720r_firmware-CVE-2021-45742 (10) -totolink -- x5000r_firmware-CVE-2021-45738 (10) -westerndigital -- my_cloud_os-CVE-2022-22992 (10)



www.sesin.at

New post from (CVE-2021-23470 (putil-merge)) has been published on

News



The Hacker News

'Roaming Mantis' Android Malware Targeting Europeans via Smishing Campaigns

A financially motivated campaign that targets Android devices and spreads its mobile malware via SMS phishing techniques since at least 2018 has spread its tentacles to strike victims located in France and Germany for the first time. Dubbed Roaming Mantis, the latest spate of activities observed in 2021 involve sending fake shipping-related texts containing a URL to a landing page from where Android



CYWARE SOCIAL
Cyware News - Latest Cyber News

Adobe Patches 13 Vulnerabilities in Illustrator

Adobe says it's not aware of any attacks exploiting these vulnerabilities. Since they all have a priority rating of "3," the company believes they are unlikely to ever be exploited.



CYWARE SOCIAL
Cyware News - Latest Cyber News

BazarBackdoor Spreads via Malicious CSV Files

Cybercriminals have found a way to abuse text-based CSV files in a phishing campaign that pretends to be Payment Remittance Advice to install BazarBackdoor malware on users' systems. In the past two days, researchers have spotted 102 actual non-sandbox corporations, along with government victims. Organizations are warned to stay aware of this threat and its techniques and prepare a defense mechanism.



ZDNet | security RSS

Brute-forcing passwords, ProxyLogon exploits were some of 2021's most popular attack methods

Log4j also became a top pick for exploitation after the discovery of a critical RCE flaw.



Blog â€" Flashpoint

[Updated] Russia Seizes Ferum, Sky-Fraud, UAS, and Trump's Dumps--and Signals More Takedowns to Come

Update as of 5:06 PM EST: Flashpoint analysts have identified the individuals that were arrested by Russian LE. One of the individuals, Artem Alexeyevich Zaytsev is listed as the CEO of Get-Net LLC, which is the registrar of the domains of Sky-Fraud, Trump's Dumps, UAS and Ferum, as well as several other domains, some of [...] The post [Updated] Russia Seizes Ferum, Sky-Fraud, UAS, and Trump's Dumps--and Signals More Takedowns to Come appeared first on Flashpoint.



SOPHOS
Naked Security

At last! Office macros from the internet to be blocked by default

It's been a long time coming, and we're not there yet, but at least Microsoft Office will be a bit safer against macro malware...



CYWARE SOCIAL
Cyware News - Latest Cyber News

BlackCat is the New Avatar of BlackMatter/DarkSide, Claims the Gang

The BlackCat ransomware, aka ALPHV, operators declared in an interview that they are former members of the DarkSide ransomware operation, leaving experts in splits. However, to everyone's surprise, BlackCat's encryptor shares no code similarities with the DarkSide/BlackMatter encryptors. Looking at rebranding efforts, experts must watch this space closely.




Threatpost

China Suspected of News Corp Cyberespionage Attack

Attackers infiltrated the media giant's network using BEC, while Microsoft moved to stop such attacks by blocking VBA macros in 5 Windows apps. Included: more ways to help stop BEC.

CISA's new JCDC worked as intended, witnesses say at Senate hearing on Log4Shell bug



CYWARE
SOCIAL
Cyware
News -
Latest Cyber
News


Chinese APT Actor Stayed Hidden for 250 Days

The xPack backdoor allowed the threat actors to remotely run WMI commands, interact with SMB shares to transfer files, and browse the web by using the backdoor as a proxy to hide their IP addresses.



IC3.gov
News


Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public



Security
Affairs

Data of +6K Puma employees stolen in December Kronos Ransomware attack


Data belonging to 6,632 Puma employees was stolen in a December 2021 ransomware attack that hit Ultimate Kronos Group (UKG). Data of 6,632 Puma employees was stolen in a ransomware attack that hit HR management platform Ultimate Kronos Group (UKG) in December. Potentially exposed data includes names, Social Security numbers, and other personal information. The [...] The post Data of +6K Puma employees stolen in December Kronos Ransomware attack appeared first on Security Affairs.



CYWARE
SOCIAL
Cyware
News -
Latest Cyber
News

Gamaredon Responsible for Attacks on Ukraine Since 2021

Microsoft shared new information on Gamaredon, also known as ACTINIUM, which has been responsible for a plethora of spear-phishing attacks against Ukrainian organizations since October 2021. One of the techniques used by Gamaredon was sending spear-phishing emails containing malicious macro as attachments that use remote templates.



CyberScoop

Inside the numbers of another big year for cyber mergers, acquisitions and investments


Sustained demand for cybersecurity services and continued innovation across the industry helped 2021 become a record-setting year for deals involving cyber companies, analysts say. The funding that flowed into cyber companies increased 136% over 2020 levels, to \$29.3 billion, up from \$12.4 billion the previous year, according to the executive summary of a report from Momentum Cyber, which advises cyber companies on mergers and acquisitions. Likewise, the total volume of mergers and acquisitions activity reached \$77.5 billion, up 294% from calendar year 2020, according to the report. Several trends are driving those numbers, analysts and executives say: Companies across the economy have expan[...]



ZDNet |
security RSS

Lazarus hackers target defense industry with fake Lockheed Martin job offers

The APT has previously masqueraded as Northrop Grumman and BAE Systems.



Krebs on
Security

Microsoft Patch Tuesday, February 2022 Edition


Microsoft today released software updates to plug security holes in its Windows operating systems and related software. This month's relatively light patch batch is refreshingly bereft of any zero-day threats, or even scary critical vulnerabilities. But it does fix four dozen flaws, including several that Microsoft says will likely soon be exploited by malware or malcontents.



CyberScoop

New York couple accused of laundering cryptocurrency from \$4.5 billion Bitfinex hack


Federal law enforcement arrested a Manhattan couple Tuesday for allegedly conspiring to launder \$4.5 billion worth of cryptocurrency stolen in a 2016 hack of virtual cryptocurrency exchange Bitfinex. The Department of Justice said it so far has seized more than \$3.6 billion in cryptocurrency tied to the hack, its largest recovery to date. The complaint accuses Ilya Lichtenstein, 34, and his wife, Heather Morgan, 31 of laundering the money over a course of five years, sometimes into their own financial accounts. The DOJ's announcement does not specify if they were allegedly involved in the initial hack itself. Justice Department officials described the arrest as a warning to criminals trying[...]



CYWARE
SOCIAL
Cyware
News -
Latest Cyber
News

Overview of the Pharmaceutical Industry Threat Landscape


The pharmaceutical industry endured a major shift in the threat landscape compared to the early stages of the pandemic from March 2020 to September 2021 as cybercriminals made it a prime target.



IT Security
Guru

Ransomware gang affiliate sentenced to 7 years


Following a guilty plea on January 31, Netwalker ransomware gang affiliate Sebastien Vachon-Desjardin was sentenced to seven years in prison for his involvement with the group by an Ontario court. Vachon-Desjardins reportedly pleaded guilty to give charges regarding "theft of computer data, extortion, the payment of cryptocurrency ransoms, and participating in the activities of a [...]" The post Ransomware gang affiliate sentenced to 7 years appeared first on IT Security Guru.



CYWARE
SOCIAL
Cyware


Russia arrests third hacking group, reportedly seizes carding forums

Authorities didn't specify what hacking groups the arrested individuals were affiliated with. However, three carding forums displayed seizure notices today claiming to be from the Russian government.



CyberScoop


Changes in federal cybersecurity leadership over the past year allowed the private and public sectors to quickly work together in responding to the disclosure of the Log4shell bug last month, experts said Tuesday at a Senate hearing. Witnesses at the Homeland Security and Governmental Affairs Committee hearing praised the usefulness of the Joint Cyber Defense Collaborative, a new center launched by the Cybersecurity and Infrastructure Security Agency in August to help federal agencies, the private sector and state and local governments collaborate on cyberthreat response. "Its structure provided a body to scramble a snap call on Saturday afternoon after Log4shell emerged to allow industry co[...]



IT Security
Guru

Cryptocurrency organisations hit with fake job offers


North Korean threat actors, known as the Lazarus group have been posting fake job listings to target the cryptocurrency vertical in the US, UK, Germany, Singapore and more. Lazarus hackers, also known as HIDDEN COBRA by the United States Intelligence Community and Zinc by Microsoft, have targeted cryptocurrency organisations in the past. The North Koreans are [...] The post Cryptocurrency organisations hit with fake job offers appeared first on IT Security Guru.



IT Security
Guru

Foreign Office hit with 'serious cyber incident'


The details emerged via a tender document published on a government website, seemingly by accident. The document stated that cyber-security firm BAE Systems Applied Intelligence was called on for "urgent support". It is thought that anonymous hackers made their way inside the FCDO systems but were detected. It is believed that no sensitive or highly [...] The post Foreign Office hit with 'serious cyber incident' appeared first on IT Security Guru.



CYWARE
SOCIAL
Cyware
News -
Latest Cyber
News

Google has auto enrolled 150 million users in 2-step verification


Google enrolled millions of users in 2-step verification after announcing the effort last year, noting in a release that it caused "the number of accounts hijacked by password theft decrease by 50%."



CYWARE
SOCIAL
Cyware
News -
Latest Cyber
News

Kimsuki APT Group Deploys Commodity RATs with Custom 'Gold Dragon' Malware

South Korean researchers have spotted a new wave of activity from the Kimsuky hacking group, involving commodity open-source remote access tools dropped with their custom backdoor, Gold Dragon.



The Hacker
News

Microsoft and Other Major Software Firms Release February 2022 Patch Updates


Microsoft on Tuesday rolled out its monthly security updates with fixes for 51 vulnerabilities across its software line-up consisting of Windows, Office, Teams, Azure Data Explorer, Visual Studio Code, and other components such as Kernel and Win32k. Among the 51 defects closed, 50 are rated Important and one is rated Moderate in severity, making it one of the rare Patch Tuesday updates without



IT Security
Guru

Molerats hackers deploy new malware


The APT group tracked as TA402 but widely known as Molerats has been observed using a new implant dubbed 'NimbleMamba'. This comes as part of a cyber-espionage campaign leveraging geofencing and URL redirects to legitimate websites. Proofpoint discovered the campaign and their analysts observed three variations of the infection chain, all targeting governments in Middle [...] The post Molerats hackers deploy new malware appeared first on IT Security Guru.



Threatpost

No Critical Bugs for Microsoft February 2022 Patch Tuesday, 1 Zero-Day


This batch had zero critical CVEs, which is unheard of. Most (50) of the patches are labeled Important, so don't delay to apply the patches, security experts said.



The Hacker
News

Palestine-Aligned Hackers Use New NimbleMamba Implant in Recent Attacks


An advanced persistent threat (APT) hacking group operating with motives that likely align with Palestine has embarked on a new campaign that leverages a previously undocumented implant called NimbleMamba. The intrusions leveraged a sophisticated attack chain targeting Middle Eastern governments, foreign policy think tanks, and a state-affiliated airline, enterprise security firm Proofpoint said



CYWARE
SOCIAL
Cyware
News -
Latest Cyber
News

Roaming Mantis Operators Use Fake SMS Messages to Lure European Targets

Researchers have detected new activity of Roaming Mantis; attackers have modified the Android trojan Wroba to target Android and iPhone users in Germany and France to steal credentials. Germany and French officials have alerted users about smishing messages with package notifications and compromised websites being used as landing pages.



The Hacker
News

Russian APT Hackers Used COVID-19 Lures to Target European Diplomats

The Russia-linked threat actor known as APT29 targeted European diplomatic missions and Ministries of Foreign Affairs as part of a series of spear-phishing campaigns mounted in October and November 2021. According to ESET's T3 2021 Threat Report shared with The Hacker News, the intrusions paved the way

<div> <div>News - Latest Cyber News</div> </div>		<div> <div>for the deployment of Cobalt Strike Beacon on compromised systems, followed by leveraging the</div> </div>
<div> <div>cyberscoop</div> <div>CyberScoop</div> </div>	<div> <div>Russian government continues crackdown on cybercriminals</div> <div>Russian authorities seized the websites of several Russian cybercrime forums Monday, the latest in a string of high-profile actions the government there has taken against cybercriminals. Visitors to the websites for Sky Fraud, a forum for stolen credit card data, were greeted with a message posted by the Russian Ministry of Internal Affairs announcing that the page was blocked. Other "carding" and cybercrime forums were also seized, including Ferum and Trump's Dumps, as well as U-A-S Shop, which offered illicit remote access to various organizations through the remote desktop protocol (RDP) tool. "The SKYFRAUD resource was closed forever during a special law enforcement operation," the messa[...]</div> </div>	<div> <div> <div>Security Affairs</div> </div> <div> <div>Russian police arrested six people involved in the theft and selling of stolen credit cards</div> <div>Russian police arrested six people individuals, allegedly members of a crime ring involved in the theft and selling of stolen credit cards. Another success of Russian police that arrested six people allegedly members of a crime gang involved in the theft and selling of stolen credit cards. The arrests were ordered by the Ministry of [...] The post Russian police arrested six people involved in the theft and selling of stolen credit cards appeared first on Security Affairs.</div> </div> </div>
<div> <div>CYWARE</div> <div>Cyware News - Latest Cyber News</div> </div>	<div> <div>SAP releases patches for ICMAD vulnerabilities, log4j issues, more</div> <div>The patches were part of a group of 19 security notes released by the company about a range of security issues. Three of the vulnerabilities were related to log4j and had a CVSS of 10.</div> </div>	<div> <div> <div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div> <div> <div>SecurityWeek Study: Over 430 Cybersecurity Mergers & Acquisitions Announced in 2021</div> <div>Financial details have been made public for 88 deals, including 11 where companies were acquired for over a billion dollars. More than 60 acquisitions involved tens or hundreds of millions of dollars.</div> </div> </div>
<div> <div>The Hacker News</div> <div>The Hacker News</div> </div>	<div> <div>Several Malware Families Using Pay-Per-Install Service to Expand Their Targets</div> <div>A detailed examination of a Pay-per-install (PPI) malware service called PrivateLoader has revealed its crucial role in the delivery of a variety of malware such as SmokeLoader, RedLine Stealer, Vidar, Raccoon, and GCleaner since at least May 2021. Loaders are malicious programs used for loading additional executables onto the infected machine. With PPI malware services such as PrivateLoader,</div> </div>	<div> <div> <div>FLASHPOINT</div> <div>Blog à€" Flashpoint</div> </div> <div> <div>Super Bowl LVI Physical Security Guide: From Counterfeiting and COVID to Protests and Phishing</div> <div>Security SEAR Level 1 The Department of Homeland Security (DHS) considers the Super Bowl a Special Event Assessment Rating (SEAR) Level 1--meaning it requires extensive federal interagency support for coordination and security from both a cyber and physical preparation standpoint. Raucous, even violent "celebrations" are just one example of the physical threats--and other potentially criminal [...] The post Super Bowl LVI Physical Security Guide: From Counterfeiting and COVID to Protests and Phishing appeared first on Flashpoint.</div> </div> </div>
<div> <div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div>	<div> <div>The Growing Menace of Malicious npm Packages</div> <div>Researchers found 1,300 malicious npm packages that could help hackers trigger supply chain attacks and steal credentials and cryptocurrency, as well as run botnets. The report states that 57% of attacks happened during three days of the week - Friday, Saturday, and Sunday. It is recommended to practice utmost caution regarding attacks that seek to abuse dependency confusion in npm.</div> </div>	<div> <div> <div>Security Affairs</div> </div> <div> <div>The Pirate Bay clones target millions of users with malware and malicious ads</div> <div>CyberNews researchers discovered five clones of The Pirate Bay serving malicious ads to more than seven million users each month. Original Post @ https://cybernews.com/security/the-pirate-bay-clones-target-millions-of-users-with-malware-and-malicious-ads/ CyberNews security researchers discovered five malicious domains masquerading as alternatives to The Pirate Bay. These domains were serving malicious ads to more than seven million users each month. Malvertising, also known [...] The post The Pirate Bay clones target millions of users with malware and malicious ads appeared first on Security Affairs.</div> </div> </div>
<div> <div>CYWARE</div> <div>Cyware News - Latest Cyber News</div> </div>	<div> <div>US Justice Department Announces \$3.6B Crypto Seizure, 2 Arrests</div> <div>Federal law enforcement officials recovered roughly \$3.6 billion in cryptocurrency linked to the hack of Bitfinex, a virtual currency exchange whose systems were breached nearly six years ago.</div> </div>	<div> <div> <div>Security Affairs</div> </div> <div> <div>US seizes \$3.6 billion worth of cryptocurrency stolen in 2016 Bitfinex hack</div> <div>The law enforcement seized \$3.6 billion worth of cryptocurrency linked to the 2016 Bitfinex cryptocurrency exchange hack. Law enforcement Ilya Lichtenstein (34) and his wife, Heather Morgan (31), were arrested for alleged conspiracy to launder \$4.5 Billion in stolen cryptocurrency stolen during the 2016 hack of Bitfinex. Law enforcement also seized over \$3.6 billion in cryptocurrency [...] The post US seizes \$3.6 billion worth of cryptocurrency stolen in 2016 Bitfinex hack appeared first on Security Affairs.</div> </div> </div>
<div> <div>eset</div> <div>WeLiveSecurity</div> </div>	<div> <div>US: Your AI has to explain its decisions</div> <div>No more turning a blind eye to algorithmic bias and discrimination if US lawmakers get their way The post US: Your AI has to explain its decisions appeared first on WeLiveSecurity</div> </div>	<div> <div> <div>Security Affairs</div> </div> <div> <div>Vodafone Portugal hit by a massive cyberattack</div> <div>A cyberattack hit Vodafone Portugal causing severe outages in the country of its communication and television services. Vodafone Portugal suffered a major cyberattack that caused service outages in the country, media reported the temporary disruption of 4G/5G communications and television services. "Vodafone was the target of a network disruption that began on the night of [...] The post Vodafone Portugal hit by a massive cyberattack appeared first on Security Affairs.</div> </div> </div>

Source: SpamHaus

Top spamming countries

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

Source: NIST

NIST CVE: Critical

CVE-2022-23329	<div> <div>A vulnerability in \${"freemarker.template.utility.Execute"?new()} of UJCMS Jspxcms v10.2.0 allows attackers to execute arbitrary commands via uploading malicious files.</div> <div> <div>CRITICAL</div> <div>Vector: network Created: 2022-02-04 Updated: 2022-02-09</div> </div> </div>	CVE-2021-43615	<div> <div>An issue was discovered in HddPassword in Insyde InsydeH2O with kernel 5.1 before 05.16.23, 5.2 before 05.26.23, 5.3 before 05.35.23, 5.4 before 05.43.22, and 5.5 before 05.51.22. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.</div> <div> <div>CRITICAL</div> <div>Vector: network Created: 2022-02-03 Updated: 2022-02-09</div> </div> </div>
CVE-2021-42554	<div> <div>An issue was discovered in Insyde InsydeH2O with Kernel 5.0 before 05.08.42, Kernel 5.1 before 05.16.42, Kernel 5.2 before 05.26.42, Kernel 5.3 before 05.35.42, Kernel 5.4 before 05.42.51, and Kernel 5.5 before</div> </div>	CVE-2021-36152	<div> <div>Apache Gobbler trusts all certificates used for LDAP connections in</div> </div>

	<p>05.50.51. An SMM memory corruption vulnerability in FvbServicesRuntimeDxe allows a possible attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.</p> <p>CRITICAL Vector: network Created: 2022-02-03 Updated: 2022-02-09</p>
CVE-2022-0365	<p>The affected product is vulnerable to an authenticated OS command injection, which may allow an attacker to inject and execute arbitrary shell commands as the Admin (root) user.</p> <p>CRITICAL Vector: network Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2021-44779	<p>Unauthenticated SQL Injection (SQLi) vulnerability discovered in [GWA] AutoResponder WordPress plugin (versions <= 2.3), vulnerable at (&listid). No patched version available, plugin closed.</p> <p>CRITICAL Vector: network Created: 2022-02-04 Updated: 2022-02-09</p>

Source: *NIST*

NIST CVE: High

CVE-2022-23330	<p>A remote code execution (RCE) vulnerability in HelloWorldAddonController.java of jpress v4.2.0 allows attackers to execute arbitrary code via a crafted JAR package.</p> <p>HIGH Vector: network Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2022-21740	<p>Tensorflow is an Open Source Machine Learning Framework. The implementation of `SparseCountSparseOutput` is vulnerable to a heap overflow. 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.</p> <p>HIGH Vector: network Created: 2022-02-03 Updated: 2022-02-09</p>

Source: *NIST*

NIST CVE: Medium

CVE-2021-45429	<p>A Buffer Overflow vulnerability exists in VirusTotal YARA git commit: 605b2edf07ed8eb9a2c61ba22eb2e7c362f47ba7 via yr_set_configuration in yara/libyara/libyara.c, which could cause a Denial of Service.</p> <p>MEDIUM Vector: local Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2021-38130	<p>A potential Information leakage vulnerability has been identified in versions of Micro Focus Voltage SecureMail Mail Relay prior to 7.3.0.1. The vulnerability could be exploited to create an information leakage attack.</p> <p>MEDIUM Vector: network Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2021-36151	<p>In Apache Gobblin, the Hadoop token is written to a temp file that is visible to all local users on Unix-like systems. This affects versions <= 0.15.0. Users should update to version 0.16.0 which addresses this issue.</p> <p>MEDIUM Vector: local Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2021-45408	<p>Open Redirect vulnerability exists in SeedDMS 6.0.15 in out.Login.php, which llows remote malicious users to redirect users to malicious sites using the "referuri" parameter.</p> <p>MEDIUM Vector: network Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2022-21741	<p>Tensorflow is an Open Source Machine Learning Framework. ### Impact An attacker can craft a TFLite model that would trigger a division by zero in the implementation of depthwise convolutions. The parameters of the convolution can be user controlled and are also used within a division operation to determine the size of the padding that needs to be added before applying the convolution. There is no check before this division that the divisor is strictly positive. 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.</p> <p>MEDIUM Vector: network Created: 2022-02-03 Updated: 2022-02-09</p>
CVE-2022-21725	<p>Tensorflow is an Open Source Machine Learning Framework. The estimator for the cost of some convolution operations can be made to execute a division by 0. The function fails to check that the stride argument is strictly positive. Hence, the fix is to add a check for the stride argument to ensure it is valid. 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.</p> <p>MEDIUM Vector: network Created: 2022-02-03 Updated: 2022-02-09</p>
CVE-2022-23568	<p>Tensorflow is an Open Source Machine Learning Framework. The implementation of `AddManySparseToTensorsMap` is vulnerable to an integer overflow which results in a `CHECK`-fail when building new `TensorShape` objects (so, an assert failure based denial of service). We are missing some validation on the shapes of the input tensors as well as</p>

	<p>Gobblin-as-a-Service. This affects versions <= 0.15.0. Users should update to version 0.16.0 which addresses this issue.</p> <p>CRITICAL Vector: network Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2021-23470	<p>This affects the package putil-merge before 3.8.0. The merge() function does not check the values passed into the argument. An attacker can supply a malicious value by adjusting the value to include the constructor property. Note: This vulnerability derives from an incomplete fix in https://security.snyk.io/vuln/SNYK-JS-PUTILMERGE-1317077</p> <p>CRITICAL Vector: network Created: 2022-02-04 Updated: 2022-02-09</p>

CVE-2021-38960	<p>IBM OPENBMC OP920, OP930, and OP940 could allow an unauthenticated user to obtain sensitive information. IBM X-Force ID: 212047.</p> <p>HIGH Vector: network Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2021-44246	<p>Totolink devices A3100R v4.1.2cu.5050_B20200504, A830R v5.9c.4729_B20191112, and A720R v4.1.5cu.470_B20200911 were discovered to contain a stack overflow in the function setNoticeCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the IpTo parameter.</p> <p>HIGH Vector: network Created: 2022-02-04 Updated: 2022-02-09</p>

CVE-2022-24249	<p>A Null Pointer Dereference vulnerability exists in GPAC 1.1.0 via the xtra_box_write function in /box_code_base.c, which causes a Denial of Service. This vulnerability was fixed in commit 71f9871.</p> <p>MEDIUM Vector: local Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2021-42059	<p>An issue was discovered in Insyde InsydeH2O Kernel 5.0 before 05.08.41, Kernel 5.1 before 05.16.41, Kernel 5.2 before 05.26.41, Kernel 5.3 before 05.35.41, and Kernel 5.4 before 05.42.20. A stack-based buffer overflow leads toarbitrary code execution in UEFI DisplayTypeDxe DXE driver.</p> <p>MEDIUM Vector: local Created: 2022-02-03 Updated: 2022-02-09</p>
CVE-2021-4043	<p>NULL Pointer Dereference in GitHub repository gpac/gpac prior to 1.1.0.</p> <p>MEDIUM Vector: local Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2021-46671	<p>options.c in atftp before 0.7.5 reads past the end of an array, and consequently discloses server-side /etc/group data to a remote client.</p> <p>MEDIUM Vector: network Created: 2022-02-04 Updated: 2022-02-09</p>
CVE-2022-23569	<p>Tensorflow is an Open Source Machine Learning Framework. Multiple operations in TensorFlow can be used to trigger a denial of service via `CHECK`-fails (i.e., assertion failures). This is similar to TFSA-2021-198 and has similar fixes. We have patched the reported issues in multiple GitHub commits. It is possible that other similar instances exist in TensorFlow, we will issue fixes as these are discovered. 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.</p> <p>MEDIUM Vector: network Created: 2022-02-03 Updated: 2022-02-09</p>
CVE-2022-21737	<p>Tensorflow is an Open Source Machine Learning Framework. The implementation of `*Bincount` operations allows malicious users to cause denial of service by passing in arguments which would trigger a `CHECK`-fail. There are several conditions that the input arguments must satisfy. Some are not caught during shape inference and others are not caught during kernel implementation. This results in `CHECK` failures later when the output tensors get allocated. 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.</p> <p>MEDIUM Vector: network Created: 2022-02-03 Updated: 2022-02-09</p>
CVE-2022-21735	<p>Tensorflow is an Open Source Machine Learning Framework. The implementation of `FractionalMaxPool` can be made to crash a TensorFlow process via a division by 0. The fix will be included in</p>

CVE-2021-41839	An issue was discovered in NvmExpressDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. Because of an Untrusted Pointer Dereference that causes SMM memory corruption, an attacker may be able to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.
	UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-09
CVE-2021-41838	An issue was discovered in SdHostDriver in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout that allows an attacker to access the System Management Mode and execute arbitrary code. This occurs because of a Numeric Range Comparison Without a Minimum Check.
	UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-09
CVE-2022-24682	An issue was discovered in the Calendar feature in Zimbra Collaboration Suite 8.8.x before 8.8.15 patch 30 (update 1), as exploited in the wild starting in December 2021. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document.
	UNRATED Vector: unkown Created: 2022-02-09 Updated: 2022-02-09
CVE-2022-0527	Cross-site Scripting (XSS) - Stored in Maven org.webjars.npm:github-com-chatwoot-chatwoot prior to 2.2.0.
	UNRATED Vector: unkown Created: 2022-02-09 Updated: 2022-02-09
CVE-2022-24694	In Mahara 20.10 before 20.10.4, 21.04 before 21.04.3, and 21.10 before 21.10.1, the names of folders in the Files area can be seen by a person not owning the folders. (Only folder names are affected. Neither file names nor file contents are affected.)
	UNRATED Vector: unkown Created: 2022-02-09 Updated: 2022-02-09
CVE-2022-24676	update_code in Admin.php in HYBBS2 through 2.3.2 allows arbitrary file upload via a crafted ZIP archive.
	UNRATED Vector: unkown Created: 2022-02-09 Updated: 2022-02-09



Source: Hybrid Analysis

Top malicious files

100% Threat score	fax_douucment (.) js
100% Threat score	CCleaner (.) v5 (.) 89 (.) 9401 (.) exe
100% Threat score	4ukey (.) exe
100% Threat score	IDMSetup (.) exe
100% Threat score	728120683066566804571311 (.) xls
100% Threat score	Truecaller-Premium-v12 (.) 12 (.) 6-Mod-AndroForever (.) com (.) apk
100% Threat score	1d44eb02e01ffe1bc26ab95b84475be288ca614a5dd0d90062f082a6c4156096 (.) exe
85% Threat score	3 (.) 0 (.) 44 (.) 1 (.) exe
85% Threat score	3 (.) 0 (.) 44 (.) 2 (.) exe
74% Threat score	æ~Ÿç«æµ·âµ-ç%oo^_1 (.) 0 (.) 10__âŽ»è´ç%oo©â°ç%oo^ (.) apk

Source: SpamHaus

Top spammers

	#1 Canadian Pharmacy A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.
	#3 Hosting Response / Michael Boehm Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.





CVE-2021-41840	An issue was discovered in NvmExpressDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout that allows an attacker to access the System Management Mode and execute arbitrary code. This occurs because of Inclusion of Functionality from an Untrusted Control Sphere.
	UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-09
CVE-2021-42113	An issue was discovered in StorageSecurityCommandDxe in Insyde 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.
	UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-09

CVE-2022-0526	Cross-site Scripting (XSS) - Stored in Maven org.webjars.npm:github-com-chatwoot-chatwoot prior to 2.2.0.
	UNRATED Vector: unkown Created: 2022-02-09 Updated: 2022-02-09

CVE-2021-37852	ESET products for Windows allows untrusted process to impersonate the client of a pipe, which can be leveraged by attacker to escalate privileges in the context of NT AUTHORITY\SYSTEM.
	UNRATED Vector: unkown Created: 2022-02-09 Updated: 2022-02-09

CVE-2022-0525	Out-of-bounds Read in Homebrew mruby prior to 3.2.
	UNRATED Vector: unkown Created: 2022-02-09 Updated: 2022-02-09

100% Threat score	Firefox Setup 91 (.) 6 (.) 0esr (.) exe
100% Threat score	92e302b598be6c149209c33b1e6d33c2
100% Threat score	king (.) exe
100% Threat score	PRJ-64779 PSS Garden _Harvest Document (.) xlsx
100% Threat score	niniteone (.) exe
100% Threat score	Your File Is Ready To Download (.) apk
87% Threat score	ZMLUVA 453DFP0021-pdf (.) exe
85% Threat score	3 (.) 0 (.) 44 (.) 0 (.) exe
77% Threat score	5d98dd8712fce37a65ae3f81362298fe8e89d9ed6030b5a88d893a06b11a49c8

	#5 RetroCubes Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.		#6 Michael Persaud Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.
	#7 Cyber World Internet Services/ e-Insites Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe.		#8 RR Media A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.
	#9 Kobeni Solutions High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US FTC in 2014.		









Source: *Hybrid Analysis*

Top malicious URL

100% Threat score	http://shrankverse(.)online/	100% Threat score	https://lnracing(.)com/wp-setting/index(.)php?blx=%24bG9yZWRhbmEuZmxvcmluZGla
100% Threat score	http://shrankverse(.)online/	100% Threat score	https://fotokeramika(.)bg/
100% Threat score	https://fotokeramika(.)bg/	100% Threat score	http://dukaree(.)com/wp-includes/6711444_861021/
100% Threat score	https://vatanproje(.)com/mo/index(.)html	100% Threat score	http://compressive(.)co(.)uk/
100% Threat score	http://rabotanakorab(.)eu/	96% Threat score	http://fotokeramika(.)bg/
96% Threat score	http://fotokeramika(.)bg/	87% Threat score	http://tour4fun(.)info/img/weather/sfx/cn/SFExpress/0526b85dfea6aa5ce0604b465c5286
86% Threat score	http://paypal-security(.)ddns(.)net/captcha	85% Threat score	https://s(.)id/W6uL
83% Threat score	http://bdinterior(.)net/	82% Threat score	http://awsd(.)publisherhunt(.)com/
79% Threat score	https://knigomania(.)bg/	77% Threat score	http://leekizer(.)com/appealinglyhh(.)php?utm_source=6e387c&%3Butm_content=cff3a
74% Threat score	https://712021(.)onlineconnects(.)xyz/link/review?uri=urn%3Aaaid%3Ascds%3AUS%3A0PS4-AGLA6T-TXG0%3Agb#464617669642e7261736368654067622e636f2e756b	72% Threat score	http://tracking(.)theoceanvillasquynhon(.)vn/tracking/click?d=fdj8ViDPH-rMrPttCteLKNb8U8uLq1cR6EeodjSBz3QlFv66K7ePTUPPrj51eGlHRKbYlfaLfVjDmqNJC1KYGh4f5VxnsWRe9zxeVgppwcL1ApIeK2ao-5t4fZwpUc6GiUBMtx9R1Pid6QoCuzYh6zKhhoLZ1Qoe01Nu2QHY7w4E6KjGX2iemkr6mY6tI
72% Threat score	http://pedagog6(.)com/	72% Threat score	http://roanokemortgages(.)com/
72% Threat score	http://tour4fun(.)info/	72% Threat score	http://url1596(.)a-dreams(.)com/ls/click?upn=NfGZJ8-2BCI1WlhWeyvdI9mJ8oIQqhBiryw2BMEU6fZz-2BQ9FQuavcZnjRXnfZ-2Fe4FhMxikiBjnZApqsefUQVla-2B4GUyR3HruCuzuFl2F2bhIaLX4rcFillPVloWMpyjC2TK4dN4d6h79q6zyxqKYOnIjGl940EIlhEQYji2ilGLoIY9hNo!2BA8GYQBqaRkQojfSj86L21ocSmCTR3L8u9w6AzzA-3D-3DnUVR_jmH3xclp7L0DeNn0TR:2FpCjvtItSN5O8XbMITOCl3aNUitaXVrJiAWnQrb9gcbYk-2BfVbVCTEmZaejMFS-2B74cxr82FdotyTQC4KeCaN-2BrFcFQyMUGBmx9AIW08zn7hVmIFTCPlnsMgMfv1baqsZdjmd6tA:2BcOhYQwAlduAWAWB9HHZu6sbdioCPNoSTlmdhFMo0a5NAQh6Bi-2BB3rtfxGbHt4huXF


Source: *SpamHaus*

Top countries with botnet

	#1 India		#2 China
	#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 Germany
	#3 Netherlands		#4 France

			
	#5 Russia		#6 Singapore
	#7 India		#8 Hong Kong
	#9 Poland		#10 Indonesia