Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

Contents

> THREAT IS A MIRROR OF SECURITY GAPS. CYBER-THREAT IS MAINLY A REFLECTION OF OUR WEAKNESSES. AN ACCURATE VISION OF DIGITAL AND BEHAVIORAL GAPS IS CRUCIAL FOR A CONSISTENT CYBER-RESILIENCE.

Patch Notes

ORACLE'S OCTOBER 2021 CPU INCLUDES 419 SECURITY PATCHES

- On Tuesday, Oracle released its latest quarterly Critical Patch Update (CPU), which includes 419 security patches for vulnerabilities across the company's portfolio.

- One of them has a CVSS score of 10 and is one of 36 that deal with critical faults. A total of 60 vulnerabilities with a CVSS score of 8 to 9 are addressed by the CPU.

GOOGLE PATCHES 19 VULNERABILITIES IN CHROME 95 BROWSER REFRESH

- Google has released an update to address multiple security flaws for the third time in less than a month. This time, the patch addresses 19 vulnerabilities, five of which are classed as "high" risk.

- If you're using Chrome, you need upgrade to version 95.0.4638.54 right away. Users of other Chromium browsers should keep an eye out for updates that address the widespread vulnerabilities.

JUNIPER NETWORKS PATCHES OVER 70 VULNERABILITIES

- Juniper Networks, a provider of networking and cybersecurity solutions, posted more than 40 security warnings this week, describing more than 70 vulnerabilities affecting the company's products.

- Approximately half of the advisories identify significant and high-severity vulnerabilities, such as those that can be used to launch denial-of-service (DoS) attacks, execute remote code (including through XSS attacks), escalate privileges, and circumvent security.

VPN PROVIDER'S MISCONFIGURATION EXPOSES ONE MILLION USERS

- A misconfigured Elasticsearch server exposed the personally identifiable information (PII) of at least one million users of a Chinese-run VPN provider.

- The researchers discovered a 100GB trove containing 500 million records, including personal information on one million users and system data on 300,000 clients.

CYBER ATTACKS

VPN

ACER HACKED TWICE IN A WEEK BY THE SAME THREAT ACTOR

- The same hacker gang that claims additional regions are vulnerable has launched a second cyberattack against Acer in less than a week.

- Acer was also the victim of another incident in March 2021, when the REvil ransomware gang encrypted their network and demanded a $50 million ransom. After the breach was verified, Acer maintained that it was a "isolated incident"...

POC EXPLOIT THAT BYPASS MACOS SECURITY IS OUT AND BEING EXPLOITED

- In macOS, the weakness can be used to overcome the three security features of file quarantine, Gatekeeper, and notarization.

- It is possible to bypass the Gatekeeper security system, which stops harmful files from being downloaded, by exploiting the vulnerability. MacOS Big Sur 11.3 and Security Update 2021-002 both address the issue.

Malware and Vulnerabilities
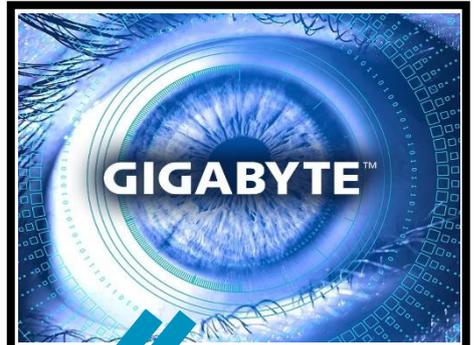
GIGABYTE ALLEGEDLY HIT BY AVOSLOCKER RANSOMWARE

- The AvosLocker ransomware gang claims to have broken into Gigabyte's network and leaked a sample of files stolen from the Taiwanese company's network. It's attempting to sell the remainder.

- The leaked documents appear to contain secret information on third-party deals as well as personally identifiable information about employees.

BUG IN POPULAR WINRAR SOFTWARE COULD LET ATTACKERS HACK YOUR COMPUTER

- A new security flaw in the WinRAR trialware file archiver programme for Windows has been discovered, which might be exploited by a remote attacker to execute arbitrary code on a targeted system.

- ARP spoofing attacks can be used to remotely launch apps, collect local host information, and even run arbitrary code by an attacker who already has access to the same network domain.

SLACK CONTAINS AN XSLEAK VULNERABILITY THAT DE-ANONYMIZES USERS

- Malicious actors can utilise a security flaw in Slack's file-sharing feature to identify users outside of the workplace chat network.

- The vulnerability, known as a cross-site leak (XSLeak), allows attackers to bypass same-origin policy, a browser security mechanism that prohibits tabs and frames from accessing each other's data.

CYBER TECH

BRAVE DITCHES GOOGLE FOR ITS OWN PRIVACY-CENTRIC SEARCH ENGINE

- Brave Browser has replaced Google as the default search engine for new users in five locations with its own no-tracking privacy-focused Brave Search.

- Brave is an open-source Chromium-based browser that prioritises user privacy by blocking advertisements and tracking scripts automatically and removes Chromium's privacy-invading features. Brave has announced that their privacy-focused Brave Search will now be the default search engine for new users in the US, Canada, and the UK.
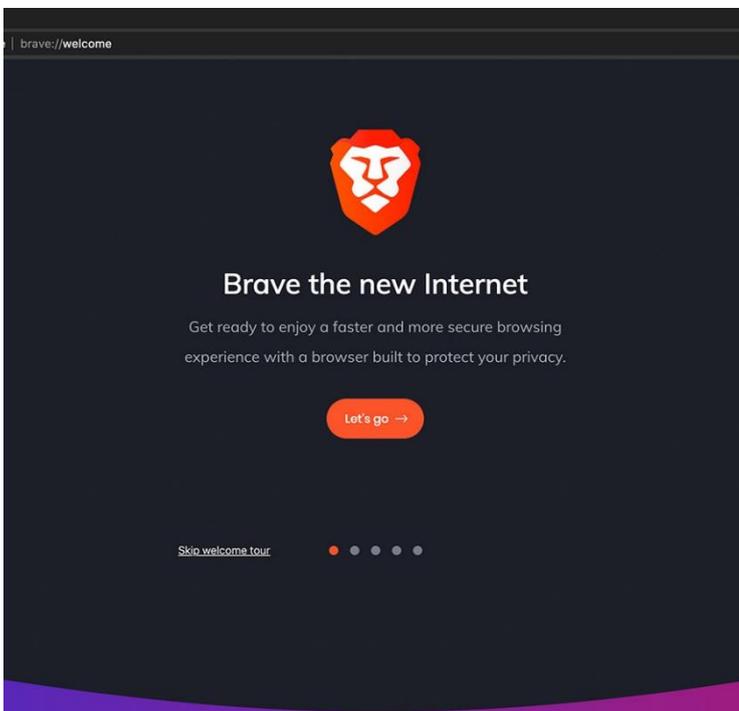
MICROSOFT REVOKES INSECURE SSH KEYS FOR AZURE DEVOPS CUSTOMERS

- Microsoft is currently pushing out Windows 10 21H2, the next edition of Windows 10, to all Windows Insiders in the Release Preview Channel in preparation for a November 2021 release.

- Windows 10, version 21H2, will include a range of features aimed at increasing productivity and security.

MICROSOFT TEAMS ADDS END-TO-END ENCRYPTION FOR ONE-TO-ONE CALLS

- End-to-end encryption (E2EE) functionality for one-to-one Microsoft Teams calls is now available as a public preview.

- Teams allows IT administrators to set up automatic recording and transcription of audio calls, in addition to encrypting data in transit and at rest. End-to-end encryption for 1:1 talks is coming to Microsoft Teams, which encrypts the real-time media flow (i.e., video and voice data) to ensure that private one-on-one conversations stay completely secret,

Infopercept

ABOUT INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

DISASTER RECOVERY AUTOMATION

In today's day and age a company's online presence and operational consistency are the central components contributing to its marketing, branding, revenue generation, information, lead generation, sales and overall business. There is little doubt then, that most companies who want to succeed in this competitive market have to invest wisely and proactively into the stability and continuation of its business's critical-function apps.

Given the importance and benefit of digital business operations for the success of a business you would ideally want it to continue unabated so that you can perform your daily business operations conveniently. Due to this, the demand for DR automation is growing as businesses are looking for ways to reduce their operational downtime. A disaster recovery plan helps you achieve this very important task, by allowing you to continue or quickly resume and kickstart important business operations and functions in the event of a disaster happening.

INVINSENSE™
Attacktical Cybersecurity Sense