INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE -08 November 2021

Contents

Patch Notes

MOZILLA DEBUTS SITE ISOLATION TECHNOLOGY WITH FIREFOX UPDATE

- Mozilla is offering improved security controls for Firefox users with the debut of a long-anticipated version of Site Isolation technology.
- Mozilla's Site Isolation offers protection from side-channel attacks, such as Spectre, through a form of process sandboxing technology. The technology protects against compromised browser rendering processes and related security risks.

CHROME 95 UPDATE PATCHES EXPLOITED ZERO-DAYS, FLAWS.

- More than a dozen Chrome vulnerabilities discovered this year have been exploited in the wild, according to data from Google's Project Zero group.
- A Chrome 95 update released by Google on Thursday patches two actively exploited Chrome vulnerabilities, as well as flaws that were disclosed recently at a Chinese hacking contest.

ANDROID PATCHES ACTIVELY EXPLOITED ZERO-DAY KERNEL BUG

- Google's Android November 2021 security updates plug 18 flaws in the framework and system components and 18 more in the kernel and vendor components.
- Among Google's November Android security updates is a patch for a zero-day weakness that "may be under limited, targeted exploitation" said Google.

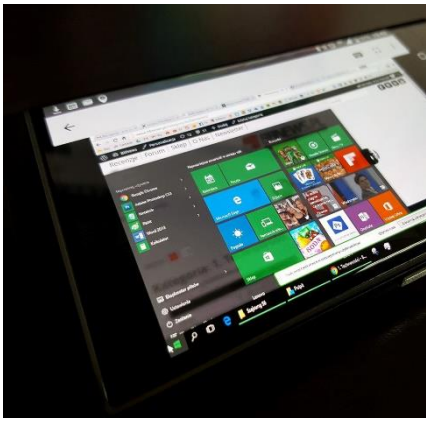
CYBER ATTACKS

HelloKitty ransomware adds DDoS attacks to extortion tactics.

- The FBI has sent out a flash alert warning private industry partners that the HelloKitty ransomware gang (aka FiveHands) has added distributed denial-of-service (DDoS) attacks to their arsenal of extortion tactics.
- The FBI said that the ransomware group would take their victims' official websites down in DDoS attacks if they didn't comply with the ransom demands.

ATTACKERS EXPLOITING GOOGLE CHROME ON WINDOWS 10 FOR UAC BYPASS

- A malware campaign has been discovered targeting Windows 10 OS running on Chrome browsers. The attackers have used a technique called User Account Control (UAC) to bypass Windows cybersecurity protections.
- Experts recommend avoiding unknown sites and clicking on suspicious links. The campaign is financially motivated and aims to steal browser credentials and cryptocurrency.



DATA BREACH AT US HEALTHCARE PROVIDER IMPACTS MORE THAN 6,500 PATIENTS

- A data breach at a physical therapy center based in the US has breached the personal data of more than 6,500 patients.
- A lot of healthcare information is leaked, including patient names, addresses, dates of birth, Social Security numbers, driver's license numbers, and medical record numbers.In a statement, the center said that it became aware of an issue in March 2021 after "suspicious emails" were sent from an employee's account.

Malware and Vulnerabilities

MICROSOFT EXCHANGE VULNERABILITIES EXPLOITED AGAIN WITH BABUK RANSOMWARE

- A malicious campaign targeting vulnerable Microsoft Exchange servers and attempting to exploit the ProxyShell vulnerability to deploy the Babuk ransomware in the victim's environment was disconver on 12 October.
- Infection typically starts with a downloader module on a victim's server.

HACKERS EXPLOITING GITLAB UNAUTHENTICATED RCE FLAW IN THE WILD

- Vulnerability in GitLab's web interface has been detected as actively exploited in the wild. Researchers warn that a large number of internet-facing GitLab instances are susceptible to attacks.
- Tracked as CVE-2021-22205, the issue relates to an improper validation of user-provided images that results in arbitrary code execution. The vulnerability, which affects all versions starting from 11.9, has since been addressed by GitLab on April 14, 2021.

LIST OF MOST COMMON HARDWARE WEAKNESSES ANNOUNCED

- MITRE and the DHS's Cybersecurity and Infrastructure Security Agency (CISA) have announced the release of the "2021 Common Weakness Enumeration (CWE) Most Important Hardware Weaknesses" list.
- The list is meant to raise awareness of common hardware weaknesses and to help prevent hardware vulnerabilities at the source, MITRE says.

APPLE MACOS VULNERABILITY ALLOWS KERNEL-LEVEL COMPROMISE

- 'Shrootless' allows bypass of System Integrity Protection IT security measures to install a malicious rootkit that goes undetected and performs arbitrary device operations.
- Researchers discovered Shrootless when, in their analysis, they came across the daemon system_installd, which has the powerful com.apple.rootless.install.heritable entitlement. With this entitlement, any child process of system_installd would be able to bypass SIP...

CYBER TECH

MICROSOFT TO RELEASE 'DEFENDER FOR BUSINESS' PLATFORM

- Microsoft announced the upcoming release of Microsoft Defender for Business, a new security tool that will soon be available for preview.
- In a blog post, Microsoft 365 product said the tool is "specially built to bring enterprise-grade endpoint security to businesses with up to 300 employees, in a solution that is easy-to-use and cost-effective."

MOZILLA DEBUTS SITE ISOLATION TECHNOLOGY WITH FIREFOX UPDATE

- Mozilla is offering improved security controls for Firefox users with the debut of a long-anticipated version of Site Isolation technology.
- Mozilla's Site Isolation offers protection from side-channel attacks, such as Spectre, through a form of process sandboxing technology. The technology protects against compromised browser rendering processes and related security risks.

CENTOS 8 EOL IS COMING CLOSE

- The difficulties around CentOS 8 involve the sudden withdrawal of official support. Official support window timeframes matter because it gives Linux users certainty that they will continue to receive bug fixes as well as patches for CVEs and security vulnerabilities that emerge.
- The official support for CentOS 8 will be curtailed by almost eight years – with end-of-life now on Dec 31, 2021 rather than the originally promised May 31, 2029.

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.

SECURITY INFORMATION & EVENT MANAGEMENT

A Business's IT network is a goldmine of information and actionable data. At Infopercept we have a strong state-of-the-art SIEM implementation plan as well as valuable market insights due to years of experience in the Cybersecurity domain. Real time log monitoring is one of the best ways to ensure business data security and integrity.

A well suited SIEM implementation ensures the ability to systematically store, create and retrieve the logs for active Monitoring, Analysis and Compliance requirements.

An SIEM brings a wide array of security functionalities that are critical for an organization's IP security.

Infopercept
SECURE • OPTIMIZE • STRENGTHEN
+91 98988 57117
sos@infopercept.com
www.infopercept.com

INVINSENSE™
Attacktical Cybersecurity Sense