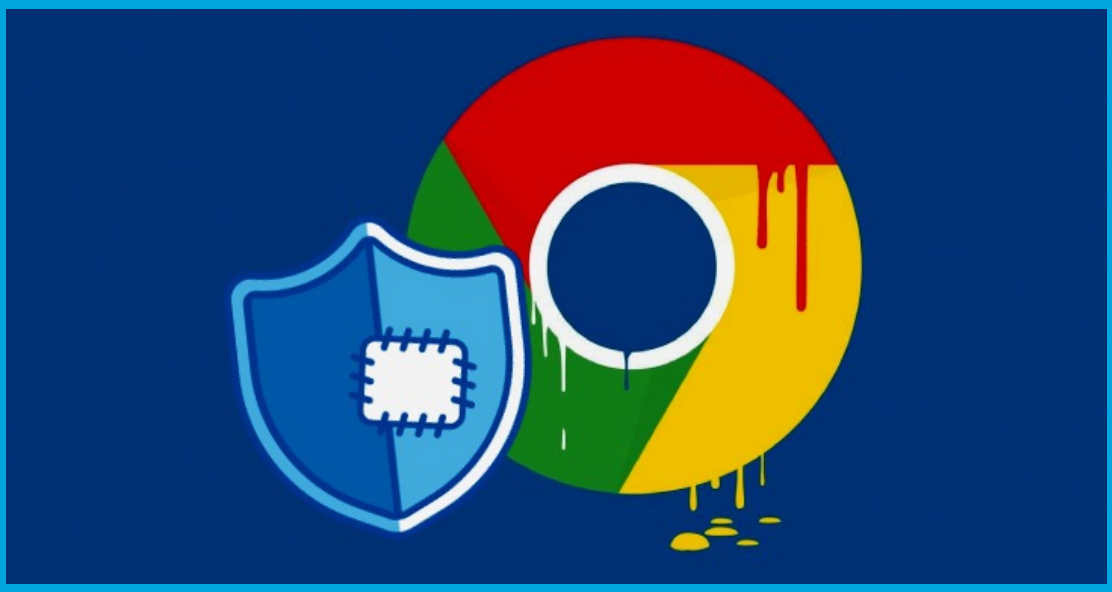
kindred

Security Newsletter

26 October 2020

Subscribe to this newsletter

New Chrome 0-day Under Active Attacks – Update Your Browser Now



Attention readers, if you are using Google Chrome browser on your Windows, Mac, or Linux computers, you need to update your web browsing software immediately to the latest version. Google released Chrome version 86.0.4240.111 to patch several security high-severity issues, including a zero-day vulnerability that has been exploited in the wild by attackers to hijack targeted computers.

Hawkes now urged other app vendors who use the same FreeType library to update their software as well, in case the threat actor decides to shift attacks against other apps.

Although the Chrome web browser automatically notifies users about the latest available version, users are recommended to manually trigger the update process by going to "Help → About Google Chrome" from the menu. The finer details about CVE-2020-15999 active exploitation attempts have not been made public. Google usually sits on technical details for months to give users enough time to update and keep even the smallest clues from falling into attackers' hands. However, since the patch for this zero-day is visible in the source code of FreeType, an open source project, it's expected that threat actors will be able to reverse-engineer the zero-day and come up with their own exploits within days or weeks.

Read More on TheHackerNews

Even More on ZDNet

French IT giant Sopra Steria hit by Ryuk ransomware

French IT services giant Sopra Steria suffered a cyberattack on October 20th, 2020, that reportedly encrypted portions of their network with the Ryuk ransomware. Sopra Steria is a European information technology company with 46,000 employees in 25 countries worldwide. The company provides a wide range of IT services, including consulting, systems integration, and software development.

A source familiar with the attack has told BleepingComputer that the Sopra Steria network was encrypted by Ryuk ransomware, the same group that infected the Universal Health Services.

This hacking group is known for its TrickBot and BazarLoader infections that allow threat actors to access a compromised network and deploy the Ryuk or Conti ransomware infections. BazarLoader is increasingly being used in Ryuk attacks against high-value targets due to its stealthy nature and is less detected than TrickBot by security software. When installed, BazarLoader will allow threat actors to remotely access the victim's computer and use it to compromise the rest of the network. After gaining access to a Windows domain controller, the attackers then deploy the Ryuk ransomware on the network to encrypt all of its devices. Those kind of attacks can be conducted swiftly and go from a single compromised machine to full company takeover in just a few hours

Read More on BleepingComputer

More #News

- ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected
- Dickey's Barbecue Pit Investigating Possible Breach Affecting 3M Payment Cards
- NSA publishes list of top vulnerabilities currently targeted by Chinese hackers
- NPM nukes NodeJS malware opening Windows, Linux reverse shells
- Elite Russian Sandworm Hackers' Epic OPSEC Problem

- Fraudsters crave loyalty points amid COVID–19
- Coinbase phishing hijacks Microsoft 365 accounts via OAuth app
- Albion Online game maker discloses data breach
- Berlin to Give Secret Services Access to Encrypted Conversations
- EU sanctions Russia over 2015 German Parliament hack
- New York financial watchdog calls for social media cybersecurity regulator after Twitter hack of Biden and Obama accounts
- How to protect your privacy when selling your phone
- BSIMM11 Observes the Cutting Edge of Software Security Initiatives
- MobileIron enterprise MDM servers under attack from DDoS gangs, nation-states
- FBI, CISA: Russian hackers breached US government networks, exfiltrated data
- Google says it mitigated a 2.54 Tbps DDoS attack in 2017, largest known to date

#Patch Time!

- WordPress deploys forced security update for dangerous bug in popular plugin
- NVIDIA patches high severity GeForce Experience vulnerabilities
- Adobe Patches 9 Vulnerabilities in Magento
- 'Active Threat' Warning: Patch Serious SharePoint Flaw Now
- Cisco Patches 17 High-Severity Vulnerabilities in Security Appliances
- Oracle's October 2020 CPU Contains 402 New Security Patches
- VMware Patches Critical Code Execution Vulnerability in ESXi
- Adobe releases another out-of-band patch, squashing critical bugs across creative software

#Tech and #Tools

- bunkerized-nginx: nginx Docker image secure by default.
- Enter The Matrix: NIST 800-30 Threat Matrix Generation tool
- Basic Buffer Overflow Guide
- DFIR Report - Ryuk From a phishing email to domain wide ransomware in 5 hours.
- How they swindle $100K without blinking an eye – Forensic Analysis of a BEC (Business Email Compromise)
- Cloud Security Tools list
- CloudSecDocs: collecting technical notes, how-tos to cloud-native technologies
- Lain Thought on End-To-End Encryption with AP Characteristics for a New Era
- Effective Practices for Cyber Incident Response and Recovery
- Project Mordor: provides pre-recorded security events to test your correlation capabilities
- MidnightTrain - Red team Persistence Framework weaponizing UEFI
- SOOTY: SOC Analysts AI-in-One Tool
- Microsoft says it took down 94% of TrickBot's command and control servers
- Barnes & Noble hit by Egregor ransomware, strange data leaked
- Google removes two Chrome ad blockers caught collecting user data
- Seven mobile browsers vulnerable to address bar spoofing attacks

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us