Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : 62264d0a Oct 13, 2021, 10:32 AM

Today's Headlines:

Leading Story

- Microsoft October 2021 Patch Tuesday: 71 Vulnerabilities, Four Zero-Days Squashed

Data Breaches & Data Leaks

- 350,000 Patients of ReproSource Fertility Diagnostics Affected by Ransomware Attack
- Oregon Eye Specialists Reports Breach of Employee Email Account

Cyber Crimes & Incidents

- Ukraine Police Cuff Botnet Herder Who Controlled 100K Machines

Vulnerabilities & Exploits

- Chinese Hackers Use Windows Zero-Day to Attack Defense, IT Firms

Trends & Reports

- Password-Stealing Attacks Surge 45% in Six Months

Privacy, Legal & Regulatory

- Russia and China Left Out of Global Anti-Ransomware Meetings

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 26, 2021, 12:00 PM Eastern

Additional Info

Leading Story

Microsoft October 2021 Patch Tuesday: 71 Vulnerabilities, Four Zero-Days Squashed

Summary

- Microsoft has released its monthly Patch Tuesday update, with 71 security fixes for software including an actively exploited zero-day bug in Win32k.

Analysis & Action

Products impacted by October's security update include Microsoft Office, Exchange Server, MSHTML, Visual Studio, and the Edge browser. The newly patched zero-day bugs are tracked as CVE-2021-40449, CVE-2021-41338, CVE-2021-40469, and CVE-2021-41335. CVE-2021-40449 is being actively exploited in an attack called MysterySnail. Issued a CVSS severity score of 7.8, this vulnerability impacts the Win32K kernel driver via a use-after-free flaw.

The three other zero-day vulnerabilities resolved in this round of patches are CVE-2021-41338, a Windows AppContainer Firewall bug that permits attackers to bypass security features; CVE-2021-40469, an RCE in Windows DNS Server; and CVE-2021-41335, an elevation of privilege bug in the Windows Kernel.

A full report of the vulnerabilities patched by Microsoft can be accessed here.

Data Breaches & Data Leaks

Premier Patient Health Care Alerts Patients About Insider Data Breach

Summary

- Premier Patient Health Care has discovered the protected health information of 37,636 patients has been obtained by an unauthorized individual in an insider incident.

Analysis & Action

On April 30, 2020, Wiseman Innovations, a technology vendor used by Premier, determined that a former Premier Patient Health Care executive had accessed its computer system in July 2020 after the termination of employment and viewed and obtained a file containing patient data. A review of the file confirmed it contained the protected health information of patients of primary care physicians.

The investigation into the breach is ongoing, but it has not been possible to date to determine what the former executive did with the file after it was acquired, although no evidence has been found to indicate any attempted or actual misuse of patient information.

As a precaution, all affected patients have been advised to be vigilant and monitor their accounts for signs of fraudulent activity

Oregon Eye Specialists Reports Breach of Employee Email Account

Summary

- Oregon Eye Specialists has discovered a breach of its email environment and the exposure of the protected health information of certain patients.

Analysis & Action

On August 10, 2021, suspicious activity was detected in an email account, prompting a password reset and investigation. The investigation confirmed an unauthorized individual had gained access to certain employee email accounts from June 29, 2021, to August 30, 2021. A review of those accounts revealed they contained protected health information such as names, dates of birth, dates of service, medical record numbers, financial information, and health insurance information, including provider name and policy number.

No evidence has been found of any actual or attempted misuse of patient data at this stage but affected individuals have been advised to monitor their accounts for suspicious activity.

Cyber Crimes & Incidents

Ukraine Police Cuff Botnet Herder Who Controlled 100K Machines

Summary

- Ukrainian law enforcement has arrested a suspected botnet herder responsible for controlling an automated network of around 100,000 compromised machines to launch DDoS and other attacks.

Analysis & Action

The Security Service of Ukraine (SSU) claimed a resident of Ivano-Frankivsk used the botnet to launch spam campaigns, scan for vulnerabilities in websites to exploit, and brute-force users' email passwords. The suspect found and communicated with customers for his services on encrypted channels like Telegram and closed underground forums and received the payment through platforms banned in Ukraine like WebMoney.

The suspect faces charges under Part 2 of Article 361-1 of the Criminal Code of Ukraine, which relates to the creation, distribution, or sale of malicious software or hardware, and interference with the work of computers, automated systems, and computer or telecoms networks.

Vulnerabilities & Exploits

Chinese Hackers Use Windows Zero-Day to Attack Defense, IT Firms

Summary

- A Chinese-speaking hacking group exploited a zero-day vulnerability in the Windows Win32k kernel driver to deploy a previously unknown remote access trojan (RAT).

Analysis & Action

The malware, known as MysterySnail, was found by Kaspersky security researchers on multiple Microsoft Servers between late August and early September 2021. They also found an elevation of privilege exploit utilizing a Win32k driver security flaw, tracked as CVE-2021-40449, that was patched by Microsoft as part of this month's Patch Tuesday.

MysterySnail can perform various tasks on infected machines, ranging from spawning new processes and killing already running ones to launching interactive shells and launching a proxy server with support for up to 50 simultaneous connections.

Further technical details and indicators of compromise can be accessed via a Kaspersky report, which can be found here.

Trends & Reports

Password-Stealing Attacks Surge 45% in Six Months

Summary

- Attacks using password-stealing malware have surged by 45% over the past six months, according to new data from Kaspersky.

Analysis & Action
The vendor analyzed several incidents of Trojan-PSW, a specialized stealer capable of gathering login and other account information. It noted 160,000 more targets in September 2021 than April, with the total number reaching nearly half a million, an increase of 45%.

Kaspersky has also seen a sharp rise in overall attempts to compromise users. It noted an increase from 24.8 million attempts in Q3 2020 to 25.5 million in the third quarter of 2021, a rise of almost 30%.

As statistics show, logins, passwords, payment details, and other personal data continue to be an attractive target for cyber-criminals and they remain a popular commodity on the dark market, explained a Kaspersky security expert.

Privacy, Legal & Regulatory

Russia and China Left Out of Global Anti-Ransomware Meetings

Summary

- The White House National Security Council is facilitating virtual meetings this week with senior officials and ministers of more than 30 countries in a virtual international counter-ransomware event to rally allies in the fight against the ransomware threat.

Analysis & Action
US President Joe Biden announced on October 1, 2021, that the U.S. would bring together allies and partners from 30 countries to join efforts to crack down on ransomware groups behind a barrage of attacks impacting organizations worldwide.

The Counter-Ransomware Initiative will meet over two days, and participants will cover everything from efforts to improve national resilience, to experiences addressing the misuse of virtual currency to launder ransom payments, our respective efforts to disrupt and prosecute ransomware criminals, and diplomacy as a tool to counter ransomware, said the President in a statement.

Even though the US and Russia have managed to resume diplomatic cooperation in several areas, Russia and China were not invited to this week's counter-ransomware meetings. An official noted that the Biden administration has observed the Russian government taking steps towards cracking down on ransomware gangs active on its territory, with more results and follow-up actions being expected in the coming months.

Reference | References

Bleeping Computer
HIPAA Journal
Bleeping Computer
Info Security Magazine
Bleeping Computer

Info Security Magazine
Health-ISAC
ZDNet
Health-ISAC
Kaspersky Labs

Tags

Daily Cyber Headlines, DCH

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.