INVINSENSE™

Attacktical Cybersecurity Sense

Infopercept

INFOPERCEPT NEWSLETTER

ISSUE -9 August 2021

Contents

"TO COMPETENTLY PERFORM RECTIFYING SECURITY SERVICE, TWO CRITICAL INCIDENT RESPONSE ELEMENTS ARE NECESSARY: INFORMATION AND ORGANIZATION.

Patches Notes

GOOGLE PATCHES SEVERAL CHROME BUGS THAT COULD BE EXPLOITED BY MALICIOUS EXTENSIONS

- Google's Chrome 92 update, which was published this week, fixes ten vulnerabilities, including three high-severity problems that resulted in tens of thousands of dollars in bug rewards for researchers.
- CVE-2021-30590 is a sandbox escape flaw that can be "exploited in conjunction with an extension or a corrupted renderer," according to the researchers. The weakness can be used by an attacker to get remote code execution outside of Chrome's sandbox.

CISCO RELEASES CRITICAL SECURITY PATCHES TO FIX BUGS IN SMALL BUSINESSES VPN ROUTER

- Cisco has released updates for serious vulnerabilities in its Small Business VPN routers that might allow a remote attacker to execute arbitrary code or cause a denial-of-service (DoS) issue.
- CVE-2021-1609 (CVSS score: 9.8) and CVE-2021-1610 (CVSS score: 7.2) are vulnerabilities in the web-based administration interface of multiple Small Business VPN Routers

PyPI PYTHON PACKAGE REPOSITORY FIXES A CRITICAL FLAW IN THE SUPPLY CHAIN.

- Last week, the maintainers of Python Package Index (PyPI) released solutions for three vulnerabilities, one of which could be exploited to gain complete control of the official third-party software repository and execute arbitrary code.
- An adversary could obtain write permission for the main branch of the "pypa/warehouse" repository, and thus execute malicious code on pypi.org, due to a flaw in the GitHub Actions workflow for PyPI's source repository named "combine-prs.yml," resulting in a scenario where an adversary could obtain write permission for the and execute malicious code on pypi.

CYBER ATTACKS

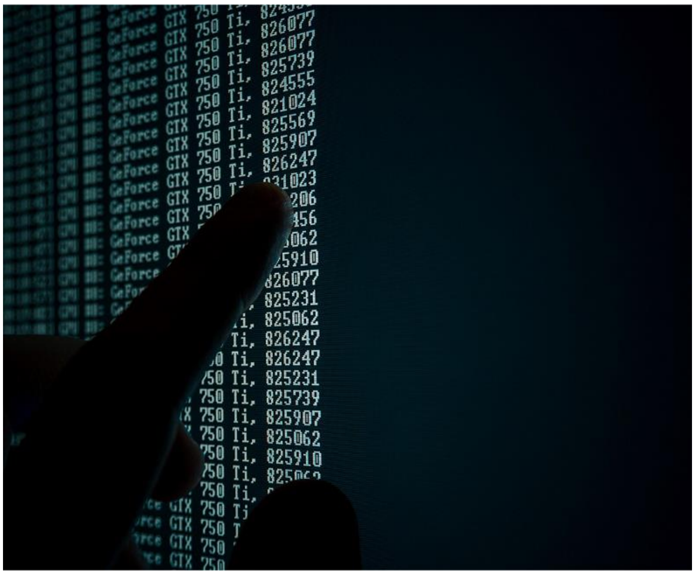
AFTER FAILED EXTORTION ATTEMPT, HACKERS LEAK EA'S DATA

- 751GB of compressed EA data including FIFA 21 source code has been leaked by hackers. According to EA, the hacked data did not include any player information.
- After collecting authentication cookies for an EA internal Slack channel from a dark web marketplace, the hackers claimed to have gotten access to the data.

PHISHING EMAILS SENT USING HACKED CHIPOTLE MARKETING ACCOUNT

Customers were offered phishing lures and malicious links that went to credential harvesting sites following a breach of the restaurant's email marketing service last month.

Between July 13 and July 16, 121 phishing emails were received from the hacked Chipotle Mailgun account. Two of the assaults used malicious voicemail message attachments, 14 impersonated USAA bank in order to acquire financial information, and the remaining 105 emails attempted to drive users to a faked Microsoft site in order to steal credentials.



MISCONFIGURED DATABASE LEAKS DATA OF OVER 60 MILLION

- Security researchers uncovered an online Elasticsearch database with the personal information of at least 63 million Americans that was entirely unsecured and exposed to the public internet.
- There were around 126 million records in the database. The number of people affected could range from 63 million to 126 million, depending on the number of duplicates found. Full names, job titles, personal email and home addresses, work email and office addresses, personal and work phone numbers, and home IP addresses were among the personally identifiable information (PII) included in the collection.

Malware and Vulnerabilities

COBALT STRIKE BUGS ALLOW TAKEDOWN OF ATTACKERS SERVERS

- Denial of service (DoS) vulnerabilities in Cobalt Strike have been uncovered, allowing for the disabling of beacon command-and-control (C2) communication channels and new deployments.

- Cobalt Strike is a legitimate penetration testing tool that may be used by red teams as an attack framework. Cobalt Strike is also used by threat actors for post-exploitation duties after deploying so-called beacons (as seen in ransomware campaigns).

MICROSOFT BROWSER BUG IS BEING EXPLOTED TO DEPLOY VBA MALWARE

- As part of an "unusual" campaign, an unidentified threat actor exploited a now-patched zero-day flaw in Internet Explorer to deliver a fully-featured VBA-based remote access trojan (RAT) capable of accessing files stored on compromised Windows systems, as well as downloading and executing malicious payloads.

- The backdoor is deployed through a fake document called "Manifest.docx" that loads the vulnerability's exploit code from an embedded template, which then executes shellcode to deploy the RAT.

MULTIPLE MALWARE FAMILIES TARGETING IIS WEB SERVERS

- A systematic analysis of attacks against Microsoft's Internet Information Services (IIS) servers has revealed as many as 14 malware families, 10 of which are new to the database, indicating that the Windows-based web server software has remained a hotbed for natively developed malware for nearly eight years.

- The study categorised over 80 malware samples into 14 distinct families (Groups 1 through 14), the majority of which were discovered for the first time between 2018 and 2021 and are still in active development.

CYBER TECH

USING LAYERED GROUP POLICY, WINDOWS ADMINISTRATORS CAN NOW RESTRICT EXTERNAL DEVICES.

- Microsoft has added layered Group Policies support, allowing IT admins to govern what internal and external devices users can install on corporate endpoints throughout their network.
- Printers, USB storage drives, and other USB peripherals added to a particular organization's restricted or approved list of devices might be denied or allowed to install on endpoints.

RESEARCHERS AT DROPBOX HAVE DEVELOPED A TOOL TO DETECT LATERAL MOVEMENT

- Hopper, a programme developed by Dropbox, UC Berkeley, and other organisations, takes a unique method to detecting hostile activities in corporate networks.
- Hopper use machine learning to detect lateral movement threats while also lowering the frequency of false security alarms, which is a major flaw in current techniques. It examines an organization's login records for indicators of lateral movement assaults.

NSA SHARES GUIDANCE ON HOW TO SECURE YOUR WIRELESS DEVICES

- The National Security System (NSS), Department of Defense (DoD), and Defense Industrial Base (DIB) teleworkers will benefit from the NSA's suggestions, which are applicable to all remote workers.
- Through Bluetooth, public Wi-Fi, and Near-Field Communications (NFC), a short-range wireless technology, cyber criminals can compromise gadgets. Personal and organisational data, passwords, and devices are all at risk as a result of this.

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.

IDENTITY ACCESS MANAGEMENT

Identity Access Management is a combination of business policies and technologies that facilitates the management of electronic digital identities. With an IAM framework in place, IT managers can control and moderate a particular user's access to critical information within an organization.

Identity and Access Management allows system administrators to utilize role-based access control. This lets the administrators assign a particular role to an individual that defines his information access scope and capabilities within an enterprise's information system or networks.

Infopercept specializes in combining all of the necessary control and tools to capture and record user login information, manage the enterprise database of user identities and orchestrate the assignment and removal of access privileges. Ensuring that the implemented IDAM solution provides a centralized directory service with monitoring as well as visibility over every aspect of an organization's user base. ↗

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

INVINSENSE™
Attacktical Cybersecurity Sense