INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE -31 Jan 2022

Contents

Patches Notes

CISCO ISSUES PATCH FOR CRITICAL RCE VULNERABILITY IN RCM FOR STAROS SOFTWARE

- Cisco Systems has released patches for a significant security hole in Cisco StarOS Software's Redundancy Configuration Manager (RCM) that could allow an unauthenticated, remote attacker to execute arbitrary code and seize control of susceptible workstations.
- In a security alert, Cisco stated, "An attacker might exploit this vulnerability by connecting to the device and browsing to the service with debug mode enabled." "If the exploit is effective, the attacker will be able to run arbitrary commands as the root user."

ORACLE TO RELEASE NEARLY 500 NEW SECURITY PATCHES

- Oracle Essbase, Graph Server and Client, Secure Backup, Communications Applications, Construction and Engineering, Enterprise Manager, Financial Services Applications, Fusion Middleware, Insurance Applications, PeopleSoft, Support Tools, and Utilities Applications will all be patched for critical vulnerabilities.
- Airlines Data Model, Big Data Graph, Communications Data Model, Commerce, Food and Beverage Applications, E-Business Suite, GoldenGate, Health Sciences Applications, HealthCare Applications, Hospitality Applications, Hyperion, iLearning, JD Edwards, MySQL, Policy Automation,

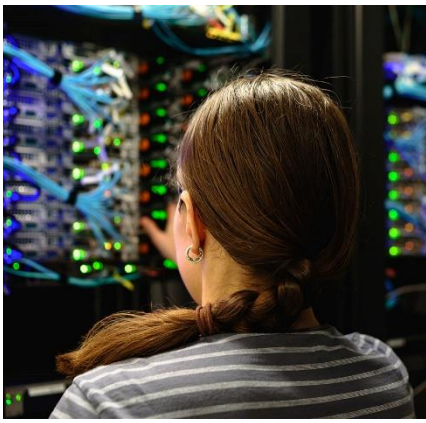
RCE BUG CHAIN PATCHED IN CENTOS WEB PANEL

- A security researcher exploited a pair of flaws in the popular web hosting platform CentOS Web Panel (CWP) to gain pre-authenticated remote command execution (RCE) as root.
- Paulos Yibelo obtained RCE but use a null binary file inclusion payload to add a malicious API key, then utilising this API key to publish to a file and including this file via the file inclusion bug.

CYBER ATTACKS

BITLOCKER ENCRYPTION: CLEAR TEXT KEY STORAGE PROMPTS SECURITY DEBATE ONLINE

- Microsoft's design choices for managing BitLocker encryption keys have been brought into question online.
- This month, there has been a Twitter and StackOverflow debate about how BitLocker cryptographic keys have been stored before consumers log in with a Microsoft account.



CHAIN OF VULNERABILITIES LED TO RCE ON CISCO PRIME SERVERS

- Two security researchers discovered a series of vulnerabilities in Cisco Prime's web interface that exposed servers to remote code execution (RCE) attacks.
- Cisco Prime is a network management service that allows you to provision, monitor, optimise, and troubleshoot wired and wireless devices.

LINUX KERNEL BUG CAN LET HACKERS ESCAPE KUBERNETES CONTAINERS

- A vulnerability in the Linux kernel identified as CVE-2022-0185 can be exploited to escape canisters in Kubernetes, granting access to host system resources.
- Security researchers warn that exploiting this security flaw is simpler and more promising than previously thought, and that patching is an urgent matter because the exploit code will soon become public.

Malware and Vulnerabilities

ZOOM VULNERABILITIES IMPACT CLIENTS, MMR SERVERS

- According to researchers, two vulnerabilities recently revealed to Zoom could have directed to remote enslavement in clients and MMR servers.
- Natalie Silvanovich, a Project Zero researcher, published an analysis of the security flaws, a outcomes of a research inspired by a zero-click attack on the videoconferencing tool illustrated at Pwn2Own.

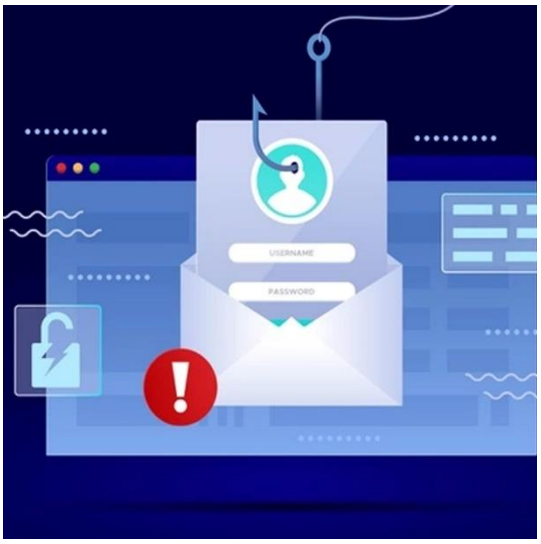
MCAFEE AGENT BUG LETS HACKERS RUN CODE WITH WINDOWS SYSTEM PRIVILEGES

- McAfee Enterprise has patched a security flaw discovered in the company's Agent software for Windows, which allowed attackers to elevate privileges and powershell with SYSTEM privileges.
- McAfee Agent is a client-side component of McAfee ePolicy Orchestrator that downloads and enforces endpoint policies as well as instals antivirus signatures, upgrades, patches, and new products on corporate endpoints.

ATTACKERS ABUSING MICROSOFT AND AWS PUBLIC CLOUD SERVICES TO SPREAD RATS

- A malicious campaign has been discovered that is spreading NetWire, Nanocore, and AsyncRAT variants while hosting them on public cloud infrastructure. Since October 2021, the campaign has been running.
- Cisco Talos discovered that the hacker group was hosting their malware on public clouds such as Microsoft and Amazon, as well as compromising dynamic DNS for C2 activities.

CYBER TECH



RESEARCHERS DISCOVER ‘EXTREMELY EASY’ 2FA BYPASS IN BOX CLOUD MANAGEMENT SOFTWARE

- Box has moved to repair a flaw in its SMS-based multi-factor authentication (MFA), just weeks after its interim one-time password (TOTP)-based MFA was discovered to be vulnerable as well.
- Varonis Threat Labs outlined how well the method could allow an attacker to use stolen information to compromise an organization's Box account and exfiltrate sensitive data without access to the victim's phone in a technical blog post.

THEPHISH: ‘THE MOST COMPLETE’ NON-COMMERCIAL PHISHING EMAIL ANALYSIS TOOL

- Security researchers now have access to a new freeware phishing email analysis tool that streamlines the entire analysis process.
- ThePhish extracts all observables from the header and body of a suspect email and creates a case on TheHive using incident response platform TheHive, observable analysis and proactive monitoring engine Cortex, and MISP.

ANDROID SECURITY TOOL APKLEAKS PATCHES CRITICAL VULNERABILITY

- A critical vulnerability that could be exploited for remote execution of arbitrary code has been patched by APKLeaks' maintainers.
- APKLeaks is open source software developed by Indonesian security engineer Dwi Siswanto that scans Android application package (APK) files for URLs, endpoints, and secrets. FirmwareDroid, a backend solution for Android firmware analysis, makes use of the application.

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.

DECEPTION TECHNOLOGY

Deception Technology is a defense practice in cybersecurity which aims to deceive attackers. This is done by the distribution of a collection of traps and decoys across your organization's systems infrastructure, in order to replicate legitimate assets.

Deception technologies have to be designed in a way to entice the attackers so that they consider it to be a worthy asset and inject a malware. Upon injection of the malware into the decoy, automated static and dynamic analysis of the injected malware is conducted and reports are automatically generated and sent to the Information Security team of your organization.

Infopercept
SECURE • OPTIMIZE • STRENGTHEN

+91 98988 57117
sos@infopercept.com
www.infopercept.com

INVINSENSE™
Attacktical Cybersecurity Sense