DoD CYBER CRIME CENTER (DC3)
DoD—Defense Industrial Base Collaborative Information Sharing Environment

10 September 2021

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles 2
Hackers Leak Passwords for 500,000 Fortinet VPN Accounts 2
Zoho Patches Actively Exploited Critical ADSelfService Plus Bug 2
GitHub Finds 7 Code Execution Vulnerabilities in 'tar' and npm CLI 2
LockBit 2.0: Ransomware Attacks Surge after Successful Affiliate Recruitment 2
Microsoft Fixes Bug Letting Hackers Take Over Azure Containers 3

Articles

Hackers Leak Passwords for 500,000 Fortinet VPN Accounts

A threat actor has leaked a list of almost 500,000 Fortinet VPN login names and passwords that were allegedly scraped from exploitable devices last summer. Yesterday, the threat actor created a post on the RAMP forum with a link to a file that allegedly contains thousands of Fortinet VPN accounts.

At the same time, a post appeared on Groove ransomware's data leak site also promoting the Fortinet VPN leak. Geographic distribution of leaked Fortinet servers Kremez told BleepingComputer that the Fortinet CVE-2018-13379 vulnerability was exploited to gather these credentials.

https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/

Zoho Patches Actively Exploited Critical ADSelfService Plus Bug

ADSelfService Plus is aimed at larger organizations that need an integrated self-service password management for and single sign-on solution for Active Directory and cloud apps. Exploits detected in the wild. The security issue is identified as CVE-2021-40539. Zoho has published a security advisory to announce that an update that patches the bug is currently available for ADSelfService Plus.

Organizations with ADSelfService Plus builds lower than 6114 are urged to apply the latest update from the developer, available using the service pack. CVE-2021-40539 is the fifth critical vulnerability reported for Zoho ManageEngine ADSelfService Plus this year.

https://www.bleepingcomputer.com/news/security/zoho-patches-actively-exploited-critical-adselfservice-plus-bug/

GitHub Finds 7 Code Execution Vulnerabilities in 'tar' and npm CLI

GitHub security team has identified several high-severity vulnerabilities in npm packages, "tar" and "@npmcli/arborist," used by npm CLI. The tar package receives 20 million weekly downloads on average, whereas arborist gets downloaded over 300,000 times every week.

The vulnerabilities affect both Windows and Unix-based users, and if left unpatched, can be exploited by attackers to achieve arbitrary code execution on a system installing untrusted npm packages. Node.js package tar remains a core dependency for installers that need to unpack npm packages post-installation. These ZIP slip vulnerabilities pose a problem for developers installing untrusted npm packages using the npm CLI, or using "tar" to extract untrusted packages.

https://www.bleepingcomputer.com/news/security/github-finds-7-code-execution-vulnerabilities-in-tar-and-npm-cli/

LockBit 2.0: Ransomware Attacks Surge after Successful Affiliate Recruitment

After a brief slowdown in activity from the LockBit ransomware gang following increased attention from law enforcement, LockBit is back with a new affiliate program, improved payloads and a change in infrastructure.

Announcing LockBit 2.0, The LockBit gang was first found advertising their affiliate program in January 2020 on a well-known, Russian-speaking forum known as XSS.]at) announcing recruitment for their LockBit 2.0 affiliate program. Each LockBit affiliate likely has its own choices of targeting, which may be targeted or opportunistic. New SamplesX-Force identified over a dozen new submissions of LockBit samples to VirusTotal occurring since the launch of the LockBit 2.0 affiliate program.

https://securityintelligence.com/posts/lockbit-ransomware-attacks-surge-affiliate-recruitment/

Microsoft Fixes Bug Letting Hackers Take Over Azure Containers

Microsoft has fixed a vulnerability in Azure Container Instances called Azurescape that allowed a malicious container to take over containers belonging to other customers on the platform. An adversary exploiting Azurescape could execute commands in the other users' containers and gain access to all their data deployed to the platform, the researchers say. When containers are deployed, ACI will isolate them from other running containers to prevent them from sharing memory space and interacting with each other. Palo Alto Networks blame it on outdated code. Researchers at Palo Alto Networks found and reported Azurescape to Microsoft. To demonstrate the attack, Palo Alto Networks published a video showing how an attacker could have broken out of their container to get administrator privileges for the entire cluster.

https://www.bleepingcomputer.com/news/security/microsoft-fixes-bug-letting-hackers-take-over-azure-containers/