مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerabilities in Various Products

Tracking #:432316203

Date:29-08-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a number of vulnerabilities have been actively exploited by malicious actors, posing significant risks to organizations.

TECHNICAL DETAILS:

A number of vulnerabilities have been actively exploited by malicious actors, posing significant risks to organizations.These vulnerabilities have been successfully leveraged to compromise systems, leading to data breaches, service disruptions, and financial losses.

Exploited Vulnerabilities:

1. **CVE-2021-33044, CVE-2021-33045-**9.8 CRITICAL- Dahua IP Camera Authentication Bypass Vulnerability-The identity authentication bypass vulnerability found in some Dahua products during the login process. Attackers can bypass device identity authentication by constructing malicious data packets.

2. **CVE-2022-0185-8.4 High-** Linux Kernel Heap-Based Buffer Overflow-A heap-based buffer overflow flaw was found in the way the legacy_parse_param function in the Filesystem Context functionality of the Linux kernel verified the supplied parameters length. An unprivileged (in case of unprivileged user namespaces enabled, otherwise needs namespaced CAP_SYS_ADMIN privilege) local user able to open a filesystem that does not support the Filesystem Context API (and thus fallbacks to legacy handling) could use this flaw to escalate their privileges on the system.

3. **CVE-2021-31196-7.2,High-** Microsoft Exchange Server Information Disclosure Vulnerability

RECOMMENDATIONS:

- Patch Systems Immediately: Apply the latest security patches and updates from software vendors to address known vulnerabilities.
- Prioritize Critical Vulnerabilities: Focus on patching vulnerabilities that are actively being exploited and pose the greatest risk to your organization.
- Conduct Vulnerability Assessments: Regularly conduct vulnerability assessments to identify and address potential weaknesses in your systems.
- Implement Strong Access Controls: Use multi-factor authentication (MFA), strong password policies, and least privilege access controls to protect sensitive data.
- Monitor Network Traffic: Use network intrusion detection and prevention systems (IDPS) to monitor network traffic for suspicious activity.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2022-0185
- https://nvd.nist.gov/vuln/detail/CVE-2021-33044
- https://nvd.nist.gov/vuln/detail/CVE-2021-33045
- https://www.cve.org/CVERecord?id=CVE-2021-31196