مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

New Attack Method Exploiting Microsoft Management Console

Tracking #:432315984

Date:26-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a novel attack technique, dubbed GrimResource, leverages specially crafted Microsoft Management Console (MMC) files to achieve full code execution on targeted systems.

TECHNICAL DETAILS:

A novel attack technique, dubbed GrimResource, leverages specially crafted Microsoft Management Console (MMC) files to achieve full code execution on targeted systems. This method exploits a vulnerability within MMC libraries and represents a significant threat as it bypasses standard security measures that block malicious macros in Office documents.

Details:

- Attack Technique: GrimResource exploits a vulnerability in MMC libraries to execute malicious code embedded within specially crafted MSC files.
- Initial Infection Vector: The attack often starts with a social engineering attempt, tricking users into opening a seemingly legitimate MSC file (e.g., disguised as "sccm-updater.msc").
- Vulnerability: The exploit leverages an unpatched XSS vulnerability within the apds.dll library (reported in late 2018).
- Code Execution: The embedded JavaScript code bypasses ActiveX warnings and potentially loads malicious payloads like Cobalt Strike.
- Impact: This attack can lead to unauthorized access, sensitive information theft, and complete system compromise

INDICATORS OF COMPROMISE(IOCs):

SHA256
4cb575bc114d39f8f1e66d6e7c453987639289a28cd83a7d802744cd99087fd7
c1bba723f79282dceed4b8c40123c72a5dfcf4e3ff7dd48db8cb6c8772b60b88
14bcb7196143fd2b800385e9b32cfacd837007b0face71a73b546b53310258bb

RECOMMENDATIONS:

- Block all threat indicators at your respective controls.
- Implement multi-layered email security controls, leveraging machine learning-based phishing detection to safeguard against malicious attachments and links.
- Update Systems: Ensure all systems are patched with the latest security updates from Microsoft, especially those addressing vulnerabilities in MMC libraries.
- Disable Scripting in MMC: Consider disabling scripting functionality within MMC (if applicable to environment) to mitigate the risk of malicious code execution.

- User Awareness: Train users to be cautious of opening unsolicited MSC files, even if they appear legitimate.
- Endpoint Detection and Response (EDR): Implement EDR solutions to detect and prevent suspicious activity related to MMC file execution.

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://www.elastic.co/security-labs/grimresource