Mphasis SOC – Information Security News
Date & Time Issued: 26-JUN-2024, 13:00 IST

Title	New attack uses MSC files and Windows XSS flaw to breach networks
Summary	• A novel command execution technique dubbed 'GrimResource' uses specially crafted MSC (Microsoft Saved Console) and an unpatched Windows XSS flaw to perform code execution via the Microsoft Management Console. • Threat actors are exploiting a novel attack technique in the wild that leverages specially crafted management saved console (MSC) files to gain full code execution using Microsoft Management Console (MMC) and evade security defenses. • After Microsoft fixed this issue in ISO files and 7-Zip added the option to propagate MoTW flags, attackers were forced to switch to new attachments, such as Windows Shortcuts and OneNote files.
Severity	Medium
Attack Vectors	• Attackers have now switched to a new file type, Windows MSC (.msc) files, which are used in the Microsoft Management Console (MMC) to manage various aspects of the operating system or create custom views of commonly accessed tools. • The researchers confirmed that the XSS flaw is still unpatched in the latest version of Windows 11. • Attackers can combine this technique with DotNetToJScript to gain arbitrary code execution, which can lead to unauthorized access, system takeover and more. • The abuse of MSC files to deploy malware was previously reported by South Korean cybersecurity firm Genian. Motivated by this research, the Elastic team discovered a new technique of distributing MSC files and abusing an old but unpatched Windows XSS flaw in apds.dll to deploy Cobalt Strike. • Elastic found a sample ('sccm-updater.msc') recently uploaded onto VirusTotal on June 6, 2024, which leverages GrimResource, so the technique is actively exploited in the wild. To make matters worse, no antivirus engines on Virus Total flagged it as malicious. • PASTALOADER retrieves a Cobalt Strike payload from the environment variables set by the VBScript, spawns a new instance of 'dllhost.exe,' and injects it using the 'DirtyCLR' technique combined with function unhooking and indirect system calls. • Attackers have developed a new technique to execute arbitrary code in Microsoft Management Console using crafted MSC files. Elastic's existing out of the box coverage shows our defense-in-depth approach is effective even against novel threats like this. Defenders should leverage our detection guidance to protect themselves and their customers from this technique before it proliferates into commodity threat groups.
Indicator of Compromise	INDICATOR TYPE: File Hash INDICATORS: • c1bba723f79282dceed4b8c40123c72a5dfcf4e3ff7dd48db8cb6c8772b60b88 • 4cb575bc114d39f8f1e66d6e7c453987639289a28cd83a7d802744cd99087fd7 • 14bcb7196143fd2b800385e9b32cfacd837007b0face71a73b546b53310258bb
Recommendations	• Block all threat indicators at your respective controls. Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Patch Management: Regularly apply security updates and patches to your Windows systems. • Ensure that all known vulnerabilities are addressed promptly. • File Handling Policies: Restrict the execution of MSC files and other potentially dangerous file types. • Implement strict file handling policies to prevent unauthorized execution. • Network Segmentation: Segment your network into zones with different security levels. Isolate critical systems from less secure areas. • Use firewalls and access controls to limit lateral movement within the network. • Behavioral Monitoring: Deploy intrusion detection systems (IDS) and security information and event management (SIEM) solutions. • Monitor abnormal behavior, especially around MMC (Microsoft Management Console) and .NET processes. • User Awareness: Educate users about the risks associated with opening unknown files or enabling macros. • Encourage a security-conscious mindset to prevent social engineering attacks. **NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**

References	• https://www.elastic.co/security-labs/grimresource • https://www.bleepingcomputer.com/news/security/new-grimresource-attack-uses-msc-files-and-windows-xss-flaw-to-breach-networks/