7 Feb 25

Cyber Threat Roundup

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

Contents

Articles

CISA Warns of Active Exploits Targeting Trimble Cityworks Vulnerability

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has warned that a security flaw impacting Trimble Cityworks GIS-centric asset management software has come under active exploitation in the wild. The vulnerability in question is CVE-2025-0994 (CVSS v4 score: 8.6), a deserialization of untrusted data bug that could permit an attacker to conduct remote code execution. This could allow an authenticated user to perform a remote code execution attack against a customer's Microsoft Internet Information Services (IIS) web server," CISA said in an advisory dated February 6, 2025. The flaw affects the following versions - Cityworks (All versions prior to 15.8.9) And Cityworks with office companion (All versions prior to 23.10). Indicators of compromise (IoCs) released by Trimble show that the vulnerability is being exploited to drop a Rust-based loader that launches Cobalt Strike and a Go-based remote access tool named VShell, among other unidentified payloads. It's currently not known who is behind the attacks, and what the end goal of the campaign is. Users running affected versions of the software are advised to update their instances to the latest version for optimal protection.

https://thehackernews.com/2025/02/cisa-warns-of-active-exploitation-in.html

Microsoft Says Attackers Use Exposed ASP.NET Keys to Deploy Malware

Microsoft warns that attackers are deploying malware in ViewState code injection attacks using static ASP. NET machine keys found online. As Microsoft Threat Intelligence experts recently discovered, some developers use ASP.NET validationKey and decryptionKey keys (designed to protect ViewState from tampering and information disclosure) found on code documentation and repository platforms in their own software. ViewState enables ASP.NET Web Forms to control state and preserve user inputs across page reloads. However, if attackers get the machine key designed to protect it from tampering and information disclosure, they can use it in code injection attacks to craft malicious payloads by attaching crafted message authentication code (MAC). This grants them remote code execution (RCE) on the targeted IIS web servers, allowing them to deploy additional malicious payloads. Microsoft has since identified over 3,000 publicly disclosed keys that could be used for these types of attacks, which are called ViewState code injection attacks.

https://www.bleepingcomputer.com/news/security/microsoft-says-attackers-use-exposed-aspnet-keys-to-deploy-malware/

Fake Google Chrome Sites Distribute ValleyRAT Malware via DLL Hijacking

Bogus websites advertising Google Chrome have been used to distribute malicious installers for a remote access trojan called ValleyRAT. The malware, first detected in 2023, is attributed to a threat actor tracked as Silver Fox, with prior attack campaigns primarily targeting Chinese-speaking regions like Hong Kong, Taiwan, and Mainland China. This actor has increasingly targeted key roles within organizations—particularly in finance, accounting, and sales department — highlighting a strategic focus on high-value positions with access to sensitive data and systems. Early attack chains have been observed delivering ValleyRAT alongside other malware families such as Purple Fox and Gh0st RAT, the latter of which has been extensively used by various Chinese hacking groups. As recently as last month, counterfeit installers for legitimate software have served as a distribution mechanism for the trojan by means of a DLL loader named PNGPlug. The latest attack sequence associated with ValleyRAT entails the use of a fake Google Chrome website to trick targets into downloading a ZIP archive containing an executable ("Setup.exe").

https://thehackernews.com/2025/02/fake-google-chrome-sites-distribute.html

Critical RCE Bug in Microsoft Outlook Now Exploited in Attacks

CISA warned U.S. federal agencies on Thursday to secure their systems against ongoing attacks targeting a critical Microsoft Outlook remote code execution (RCE) vulnerability. Discovered by Check Point vulnerability researcher Haifei Li and tracked as CVE-2024-21413, the flaw is caused by improper input validation when opening emails with malicious links using vulnerable Outlook versions. The attackers gain remote code execution capabilities because the flaw lets them bypass the Protected View (which should block harmful content embedded in Office files by opening them in read-only mode) and open malicious Office files in editing mode. When it patched CVE-2024-21413 one year ago, Microsoft also warned that the Preview Pane is an attack vector, allowing successful exploitation even when previewing maliciously crafted Office documents. This security flaw (dubbed Moniker Link) lets threat actors bypass built-in Outlook protections for malicious links embedded in emails using the file:// protocol and by adding an exclamation mark to URLs pointing to attacker-controlled servers. CVE-2024-21413 affects multiple Office products, including Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise, Microsoft Outlook 2016, and Microsoft Office 2019, and successful CVE-2024-21413 attacks can result in the theft of NTLM credentials and the execution of arbitrary code via maliciously crafted Office documents.

https://www.bleepingcomputer.com/news/security/critical-rce-bug-in-microsoft-outlook-now-exploited-in-attacks/

Lazarus Group Targets Organizations with Sophisticated LinkedIn Recruiting Scam

Bitdefender Labs warns of an active campaign by the North Korea-linked Lazarus Group, targeting organizations by capturing credentials and delivering malware through fake LinkedIn job offers. TThe threat actors' infection chain is complex, containing malicious software written in multiple programming languages and using a variety of technologies, such as multi-layered Python scripts that recursively decode and execute themselves, a JavaScript stealer that first harvests browser data before pivoting to further payloads, and.NET-based stagers capable of disabling security tools, configuring a Tor proxy, and launching crypto miners. The malware infects Windows, macOS, and Linux via cross-platform compatibility, uses a variety of exfiltration methods (HTTP, Tor, and attacker-controlled IPs), and includes modules for keylogging, system reconnaissance, file harvesting, and continuous C2 communication, demonstrating the breadth and complexity of its capabilities.

https://www.bitdefender.com/en-us/blog/labs/lazarus-group-targets-organizations-with-sophisticated-linkedin-recruiting-scam