

Federal agency hacked by 2 groups thanks to flaw that went unpatched for 4 years

Getty Images

reader comments

39 with

Share this story

Multiple threat actors—one working on behalf of a nation-state—gained access to the network of a US federal agency by exploiting a four-year-old vulnerability that remained unpatched, the US government warned.

Exploit activities by one group likely began in August 2021 and last August by the other, according to an advisory jointly published by the Cybersecurity and Infrastructure Security Agency, the FBI, and the Multi-State Information Sharing and Analysis Center. From last November to early January, the server exhibited signs of compromise.

Vulnerability not detected for 4 years

Both groups exploited a code-execution vulnerability tracked as CVE-2019-18935 in a developer tool known as the Telerik user interface (UI) for ASP.NET AJAX, which was located in the agency's Microsoft Internet Information Services (IIS) web server. The advisory didn't identify the agency other than to

say it was a Federal Civilian Executive Branch Agency under the CISA authority.

The Telerik UI for ASP.NET AJAX is sold by a company called Progress, which is headquartered in Burlington, Massachusetts, and Rotterdam in the Netherlands. The tool bundles more than 100 UI components that developers can use to reduce the time it takes to create custom Web applications. In late 2019, Progress released version 2020.1.114, which patched CVE-2019-18935, an insecure deserialization vulnerability that made it possible to remotely execute code on vulnerable servers. The vulnerability carried a severity rating of 9.8 out of a possible 10. In 2020, the NSA warned that the vulnerability was being exploited by Chinese state-sponsored actors.

“This exploit, which results in interactive access with the web server, enabled the threat actors to successfully execute remote code on the vulnerable web server,” Thursday’s advisory explained. “Though the agency’s vulnerability scanner had the appropriate plugin for CVE-2019-18935, it failed to detect the vulnerability due to the Telerik UI software being installed in a file path it does not typically scan. This may be the case for many software installations, as file paths widely vary depending on the organization and installation method.”

Advertisement

More unpatched vulnerabilities

To successfully exploit CVE-2019-18935, hackers must first have knowledge of the encryption keys used with a component known as the Telerik RadAsyncUpload. Federal investigators suspect the threat actors exploited one of two vulnerabilities discovered in 2017 that also remained unpatched on the agency server.

Attacks from both groups used a technique known as DLL side

loading, which involves replacing legitimate dynamic-link library files in Microsoft Windows with malicious ones. Some of the DLL files the group uploaded were disguised as PNG images. The malicious files were then executed using a legitimate process for IIS servers called w3wp.exe. A review of antivirus logs identified that some of the uploaded DLL files were present on the system as early as August 2021.

The advisory said little about the nation-state-sponsored threat group, other than to identify the IP addresses it used to host command-and-control servers. The group, referred to as TA1 in Thursday's advisory, began using CVE-2019-18935 last August to enumerate systems inside the agency network. Investigators identified nine DLL files used to explore the server and evade security defenses. The files communicated with a control server with an IP address of 137.184.130[.]162 or 45.77.212[.]12. The traffic to these IP addresses used unencrypted Transmission Control Protocol (TCP) over port 443. The threat actor's malware was able to load additional libraries and delete DLL files to hide malicious activity on the network.

The advisory referred to the other group as TA2 and identified it as XE Group, which researchers from security firm Volexity have said is likely based in Vietnam. Both Volexity and fellow security firm Malwarebytes have said the financially motivated group engages in payment-card skimming.

"Similar to TA1, TA2 exploited CVE-2019-18935 and was able to upload at least three unique DLL files into the C:\Windows\Temp\ directory that TA2 executed via the w3wp.exe process," the advisory stated. "These DLL files drop and execute reverse (remote) shell utilities for unencrypted communication with C2 IP addresses associated with the malicious domains."

The breach is the result of someone in the unnamed agency failing to install a patch that had been available for years.

As noted earlier, tools that scan systems for vulnerabilities often limit their searches to a certain set of pre-defined file paths. If this can happen inside a federal agency, it likely can happen inside other organizations.

Anyone using the Telerik UI for ASP.NET AJAX should carefully read Thursday's advisory as well as the one Progress published in 2019 to ensure they're not exposed.

<https://arstechnica.com/?p=1924743>