Hackers actively exploit high-severity networking vulnerabilities

reader comments

31 with 27 posters participating

Share this story

Hackers are actively exploiting two unrelated high-severity vulnerabilities that allow unauthenticated access or even a complete takeover of networks run by Fortune 500 companies and government organizations.

The most serious exploits are targeting a critical vulnerability in F5's Big-IP advanced delivery controller, a device that's typically placed between a perimeter firewall and a Web application to handle load balancing and other tasks. The vulnerability, which F5 patched three weeks ago, allows unauthenticated attackers to remotely run commands or code of their choice. Attackers can then use their control of the device to hijack the internal network it's connected to.

Prescient

The presence of a remote code execution flaw in a device located in such a sensitive part of a network gave the vulnerability a maximum severity rating of 10. Immediately after F5 released a patch on June 30, security practitioners predicted that the flaw—which is tracked as CVE-2020-5902—would be exploited against any vulnerable

networks that didn’t quickly install the update. On Friday, the US Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory that proved those warnings prescient.

“CISA has conducted incident response engagements at US Government and commercial entities where malicious cyber threat actors have exploited CVE-2020-5902—an RCE vulnerability in the BIG-IP Traffic Management User Interface (TMUI)—to take control of victim systems,” the advisory stated.

Officials continued:

> *CISA has observed scanning and reconnaissance, as well as confirmed compromises, within a few days of F5’s patch release for this vulnerability. As early as July 6, 2020, CISA has seen broad scanning activity for the presence of this vulnerability across federal departments and agencies—this activity is currently occurring as of the publication of this Alert.*
>
> *CISA has been working with several entities across multiple sectors to investigate potential compromises relating to this vulnerability. CISA has confirmed two compromises and is continuing to investigate. CISA will update this Alert with any additional actionable information.*

Et tu, Cisco?

Attackers are exploiting a second vulnerability found in two network products sold by Cisco. Tracked as CVE-2020-3452, the path-traversal flaw resides in the company’s Adaptive Security Appliance and Firepower Threat Defense systems. It allows unauthenticated people to remotely view sensitive files that, among other things, can disclose WebVPN configurations, bookmarks, Web cookies, partial Web content, and HTTP URLs. Cisco issued a patch on Wednesday. A day later, it updated its

advisory.

“Cisco has become aware of the availability of public exploit code and active exploitation of the vulnerability that is described in this advisory,” the update said. “Cisco encourages customers with affected products to upgrade to a fixed release as soon as possible.”

Proof-of-concept code began circulating almost immediately after Cisco issued the fix, setting off a race between attackers and defenders.

The impact of these vulnerabilities—particularly the one affecting F5 customers—is serious. These in-the-wild attacks provide ample reason to occupy the weekend of any IT administrators who have yet to patch their vulnerable systems.

https://arstechnica.com/?p=1694402