The attacks include at least one campaign to distribute ransomware, and another in which a threat actor appears to be creating admin users on vulnerable TeamCity instances for potential future use.

One of the vulnerabilities (identified as CVE-2024-27198) has a near-maximum severity CVSS rating of 9.8 out of 10 and is an authentication bypass issue in TeamCity's Web component. Researchers from Rapid7 who discovered the vulnerability and reported it to JetBrains have described it as enabling a remote unauthenticated attacker to execute arbitrary code to take complete control of affected instances.

CVE-2024-27199, the other vulnerability that JetBrains disclosed, is a moderate-severity authentication bypass flaw in the same TeamCity Web component. It allows for a "limited amount" of information disclosure and system modification, according to Rapid7.

TeamCity Developers: A Valuable Target for Attackers

Some 30,000 organizations use TeamCity to automate build, testing and deployment processes for software projects in CI/CD environments. Like other recent TeamCity flaws — such as CVE-2024-23917 in February 2024, and CVE-2023-42793, which Russia's Midnight Blizzard group used in attacks last year (it is also known for the infamous SolarWinds supply chain attacks), the two new ones have stoked considerable concern.

The worries have to do with the potential for attackers to abuse the flaws to take control of an organization's software builds and projects to launch mass supply chain attacks.

"Attackers are realizing that tools like TeamCity for configuration deployment are an easy way to rapidly propagate malicious code," says Greg Fitzgerald, co-founder of Sevco Security. Many also use trusted tools like TeamCity to enable lateral movement on a mass scale, he says.

Stephen Fewer, principal security researcher at Rapid7, says that armed with the new vulnerabilities, an attacker can use search engines like Shodan and FOFA to locate exposed TeamCity servers. One caveat is that there a high number of honeypot servers masquerading as TeamCity servers, so bad actors might need to do some extra work to find legitimate instances, he says.

Exploitation after discovery is trivial, Fewer says. "CVE-2024-27198, can be leveraged via a single HTTP request," he says. This allows "an attacker to create a new administrator user account or access token on the system, and from there the attacker can leverage this to completely take over the server, including remote code execution [RCE] on the target operating system."

By creating a new admin account on a vulnerable instance, an attacker can potentially access and modify all the resources that the TeamCity instances manages, including projects, build agents, and artifacts.

"Another avenue the attacker can employ is to leverage their access to run arbitrary commands on the underlying operating system to take full control over the server," Fewer says. One way to do this is by deploying a malicious TeamCity plug-in that hosts a payload of the attacker's choice. Another option is to leverage a REST API for debugging purposes that is available in some versions of TeamCity to run commands on the operating system. "From here, the attack may pivot deeper into the target's network, or establish persistence on the compromised server to maintain access," Fewer says.

High-Severity JetBrains TeamCity Threats

On March 5, the director of CrowdStrike's threat hunting group reported observing multiple instances in which a threat actor had exploited the two flaws to deploy what appeared to be a modified version of Jasmin, an open source tool that red-team testers can use to simulate a real ransomware attack. Its maintainers have described Jasmin as a WannaCry clone.

Separately, LeakIX, a site that aggregates breach and leak data, reported detecting some 1,711 exposed TeamCity instances on the Web, of which 1,442 showed signs of someone having created rogue user accounts on them via CVE-2024-27198. "If you were/are still running a vulnerable system, assume compromise," LeakIX noted on X, the platform formerly known as Twitter.

Meanwhile, the nonprofit Internet-monitoring site ShadowServer.org reported observing exploitation activity for CVE-2024-27198 starting Mar 4 — a day after JetBrains disclosed the flaw.

"If running JetBrains TeamCity on-prem — make sure to patch for latest CVE-2024-27198 (remote auth bypass) & CVE-2024-27199 vulns NOW!," Shadowserver warned. The volunteer-based cyber threat intelligence organization reported detecting 1,182 instances of TeamCity, some of which might have a patch in place already. It identified the top affected countries as the US with 298 instances, and Germany with 188.

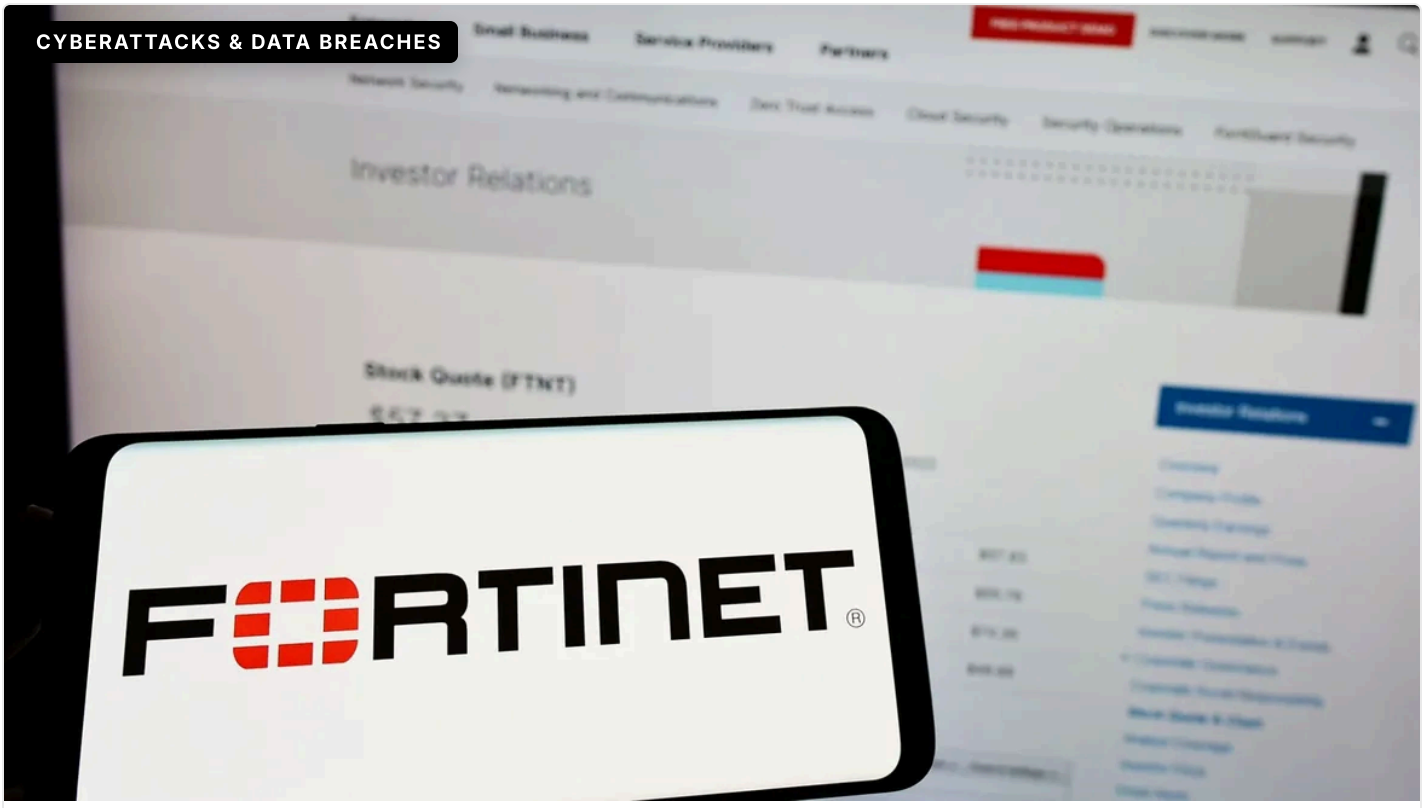
About the Author

Jai Vijayan

Contributing Writer

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year career at Computerworld, Jai...

You May Also Like



Critical Fortinet Flaws Under Active Attack

by Jai Vijayan, Contributing Writer

DEC 17, 2025

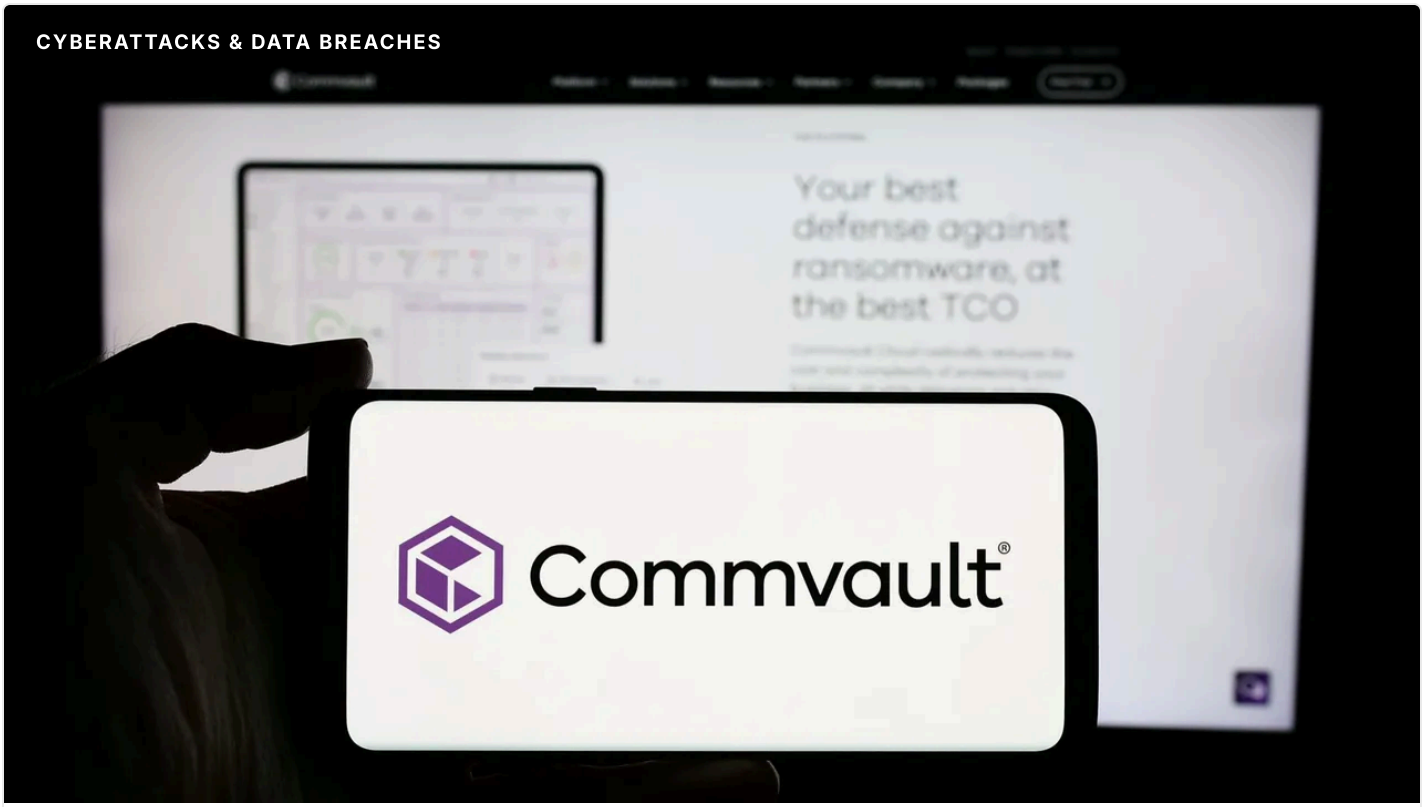
F5 BIG-IP Environment Breached by Nation-State Actor

by Alexander Culafi

Jaguar Land Rover Shows Cyberattacks Mean (Bad) Business

by Robert Lemos, Contributing Writer

CYBERATTACKS & DATA BREACHES



Researcher Says Patched Commvault Bug Still Exploitable

by Jai Vijayan, Contributing Writer

MAY 06, 2025