CISA Warns of Exploited Flaws in Cisco, Microsoft, Hitachi & Progress

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added five security vulnerabilities affecting Cisco, Hitachi Vantara, Microsoft Windows, and Progress WhatsUp Gold to its Known Exploited Vulnerabilities (KEV) catalog. This action signals that these flaws are actively exploited in the wild, posing significant risks to affected systems.

One of the vulnerabilities, **CVE-2023-20118**, affects Cisco Small Business RV Series Routers. This command injection flaw exists in the router's web-based management interface, allowing authenticated remote attackers to gain root-level privileges and access sensitive data. Cisco has not provided a fix since these routers have reached their end-of-life status, leaving organizations vulnerable.

Two security flaws in the Hitachi Vantara Pentaho BA Server, **CVE-2022-43939** and **CVE-2022-43769**, have also been flagged. The first vulnerability arises from an authorization bypass issue, enabling attackers to access resources through non-canonical URL paths. The second flaw allows attackers to inject malicious Spring templates into configuration files, leading to arbitrary command execution. Both issues were addressed in security updates released in August 2024.

An older vulnerability, **CVE-2018-8639**, affecting Microsoft Windows Win32k, has resurfaced as an active threat. This flaw, which allows local privilege escalation through improper resource handling, was initially patched in December 2018 but is still targeted in modern attack campaigns.

Another high-risk vulnerability, **CVE-2024-4885**, affects

Progress WhatsUp Gold, a widely used network monitoring software. This path traversal vulnerability enables unauthenticated, remote attackers to execute arbitrary code on affected systems. The flaw was patched in June 2024 with version 2023.1.3, but ongoing exploitation attempts have been observed.

C**VE-2023-20118** is being leveraged to conscript vulnerable Cisco routers into a botnet called PolarEdge. At the same time, the exploitation of CVE-2024-4885 has been detected globally. Security researchers from the Shadowserver Foundation and GreyNoise report that attack attempts have originated from Hong Kong, Russia, Brazil, South Korea, and the United Kingdom.

CISA has identified active exploitation of vulnerabilities. To ensure their systems are safeguarded, they have mandated that Federal Civilian Executive Branch (FCEB) agencies implement mitigations by March 24, 2025. Organizations using affected products are strongly urged to take action. They should apply the latest patches or implement alternative security measures, which will help prevent potential attacks.