Security Bulletin Update

To: All Bomgar Customers

From: ScreenMeet

Date: January 13, 2025

Subject: US Treasury Hacked through exploitation of Command Injection Vulnerability in Bomgar/ Beyond Trust (Reuters Article)

Whether you are running a self-hosted or SaaS version of Bomgar, you are at risk of on-going security vulnerabilities due to the outdated security model of that platform.

Technical Background

"A compromised Remote Support SaaS API key was identified, which allowed for password resets of local application accounts, and was promptly revoked," the security bulletin said.

In updates published earlier this week, BeyondTrust disclosed two vulnerabilities in its Privileged Remote Access and Remote Support tools. The first is a medium-severity vulnerability tracked as CVE-2024-12686. The second is a high-severity flaw tracked as CVE-2024-12356, which received a CVSS score of 9.8 out of 10.

However, CISA on Thursday (12/17/24) added CVE-2024-12356 to its Known Exploited Vulnerabilities catalog. BeyondTrust's advisory warned that exploitation of CVE-2024-12356 could "allow an unauthenticated attacker to inject commands that are run as a site user."

The Solution

ScreenMeet is built around principles of zero-trust. Multiple layers of authentication are required to execute any kind of code on the remote endpoint. First, all users must be authenticated via a 3rd party like Salesforce or ServiceNow and possess the appropriate privileges via role based access in these platforms. From there, users can launch an interactive remote support session on the endpoint via ScreenMeet if they have the required privileges to do so. Furthermore, ScreenMeet does not add any additional local users or profiles to remote devices, nor does it open any inbound network ports.

Contact your ScreenMeet Sales Rep (sales@screenmeet.com) today to learn more.