Alert Bulletin

Bulletin N.: 2024-38
Publication Date: 20/09/2024
Subject: Alert 2024-38 Critical Vulnerability in Veeam Backup & Replication CVE-2024-40711
Traffic Light Protocol (TLP): White

Affected Product(s):

- Veeam Backup & Replication versions 12.1.2.172 and earlier.

Description:

Veeam recently disclosed a critical remote code execution (RCE) vulnerability identified as CVE-2024-40711. This flaw affects Veeam Backup & Replication (VBR) in versions 12.1.2.172 and earlier. The vulnerability allows unauthenticated attackers to execute arbitrary code on vulnerable systems, potentially compromising an organization's entire infrastructure. Due to the critical role VBR plays in enterprise data protection, it is a potential target for ransomware operators. Veeam has released an update to address this issue and recommends users immediately update to version 12.2.0.334.

While proof-of-concept (PoC) exploits have been reported on GitHub, security researchers have opted not to release the full exploitation details due to the vulnerability's significance for malware operators. Exploitation of this flaw could lead to lateral movement within the network and the compromise of the entire infrastructure. Organizations using VBR are urged to apply the updates as soon as possible.