Posting Date: 2026/09/03

Vulnerability Alert2 Critical Security Vulnerabilities Exist in Veeam ONE 13.1

- Subject: Vulnerability Alert2 Critical Security Vulnerabilities Exist in Veeam ONE 13.1

- Content:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202608-00000022
  - Veeam ONE is used for monitoring local Veeam backup infrastructure. Recently, Veeam released security advisories for critical vulnerabilities (CVE-2026-64633, CVSS 4.x: 10.0 and CVE-2026-65641, CVSS 4.x: 9.3). CVE-2026-64633 allows an unauthenticated attacker to execute code remotely on agent hosts; CVE-2026-65641 allows an unauthenticated attacker to force service accounts to perform SMB authentication.
- Affected Platforms:
  - Veeam ONE version 13.0.2.6723 and earlier versions
  - Veeam ONE version 13.1.0.7034 and earlier versions
- Recommendations:
  - Please update to the following versions:
  - CVE-2026-64633 Veeam ONE 13.1 (build 13.1.0.7034), Veeam ONE 13.0.2 Patch 1 (build 13.0.2.7159)
  - CVE-2026-65641 Veeam ONE 13.1 Patch 0 (build 13.1.0.7233), Veeam ONE 13.0.2 Patch 1 (build 13.0.2.7159)
- References:
  1. https://www.veeam.com/kb4892
  2. https://www.veeam.com/kb4905
  3. https://nvd.nist.gov/vuln/detail/CVE-2026-64633
  4. https://nvd.nist.gov/vuln/detail/CVE-2026-65641

Computer and Communication Center
Network System Division Respectfully