

Date Posted: 2026/08/07

[Vulnerability Alert]Two Critical Security Vulnerabilities in Veeam Service Provider Console

- Subject: [Vulnerability Alert]Two Critical Security Vulnerabilities in Veeam Service Provider Console
- Description:
 - Forwarded Security Alert from TWCERT/CC (Taiwan Computer Emergency Response Team/Coordination Center) TWCERTCC-200-202608-00000006
 - Backup and data protection software vendor Veeam's remote management console, Veeam Service Provider Console (VSPC), is a tool used for remote monitoring and management across on-premises and cloud application environments. Recently, the vendor provided patches for high-risk security vulnerabilities (CVE-2026-58073, CVSS 4.x: 9.5 and CVE-2026-58072, CVSS 4.x: 9.0). CVE-2026-58073 allows an unauthenticated attacker to impersonate a managed agent and obtain its credentials; CVE-2026-58072 allows arbitrary file writes to the management server, which could lead to remote code execution.
- Affected Platforms:
 - Veeam Service Provider Console version 9, Veeam Service Provider Console 9.2.1.33875
- Recommendations:
 - Please update Veeam Service Provider Console to version 9.3.0.35057 or later
- Reference Information:
 1. <https://www.veeam.com/kb4893>
 2. <https://nvd.nist.gov/vuln/detail/CVE-2026-58073>
 3. <https://nvd.nist.gov/vuln/detail/CVE-2026-58072>

Computer and Communication Center
Network Systems Division

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260807_27



Last update: **2026/08/07 10:22**