Landesamt für Sicherheit in der Informationstechnik

Veeam Backup & Replication: Mehrere Schwachstellen

CVSS Base Score	Meldung	Datum	Stand
10.0 (kritisch)	LSI-SEC-2024-2057	05.09.2024	**05.09.2024**
CVSS Temporal Score			
8.7 (hoch)			

Betroffene Systeme

Betriebssystem

- Sonstiges

Produktbeschreibung

Veeam Backup & Replication ist eine Datensicherungslösung für VMware vSphere- und Microsoft Hyper-V-Umgebungen.

Software

05.09.2024

- Veeam Backup & Replication < 12.2.0.334

Angriff

Angriff

Ein Angreifer kann mehrere Schwachstellen in Veeam Backup & Replication ausnutzen, um Dateien zu manipulieren, erweiterte Rechte zu erlangen, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen preiszugeben.

CVE

CVE-2024-39718

Es besteht eine Schwachstelle in Veeam Backup & Replication. Diese Sicherheitslücke ermöglicht das Löschen von Dateien mit denselben Berechtigungen wie das Dienstkonto. Ein entfernter, authentisierter Angreifer mit geringen Rechten kann diese Sicherheitslücke ausnutzen, um Dateien zu Löschen.

CVSS v3.1 Base Score: 8.1 / Temporal Score: 7.1
AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:X (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?version=3.1&vector=AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:X)

CVE-2024-40710

Es besteht eine Schwachstelle in Veeam Backup & Replication. Diese Sicherheitslücke wird derzeit nicht im Detail beschrieben. Ein entfernter, authentisierter Angreifer kann diese Schwachstellen zur Ausführung von beliebigem Code ausnutzen.

CVSS v3.1 Base Score: 8.8 / Temporal Score: 7.7
AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:X (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?version=3.1&vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:X)

CVE-2024-40712

Es besteht eine Schwachstelle in Veeam Backup & Replication aufgrund eines Path Traversal Fehlers. Ein lokaler Angreifer kann diese Schwachstelle ausnutzen, um erweiterte Rechte zu erlangen.

CVSS v3.1 Base Score: 7.8 / Temporal Score: 6.8
AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:X (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?version=3.1&vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:X)

CVE-2024-40713

Es besteht eine Schwachstelle in Veeam Backup & Replication aufgrund eines Fehlers, der die Änderung von MFA-Einstellungen ermöglicht. Ein lokaler Angreifer kann diese Schwachstelle ausnutzen, um die Multi-Faktor-Authentifizierung zu umgehen.

CVSS v3.1 Base Score: 7.8 / Temporal Score: 6.8
AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:X (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?version=3.1&vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:X)

CVE-2024-40714

Es besteht eine Schwachstelle in Veeam Backup & Replication. Diese Sicherheitslücke besteht aufgrund einer unsachgemäßen Validierung des TLS-Zertifikats, was zum Abfangen vertraulicher Anmeldeinformationen während Wiederherstellungsvorgängen führt. Ein entfernter, anonymer Angreifer kann diese Schwachstelle ausnutzen, um vertrauliche Informationen preiszugeben. Zur erfolgreichen Ausnutzung ist eine Benutzeraktion erforderlich.

CVSS v3.1 Base Score: 8.3 / Temporal Score: 7.2
AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:X (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?version=3.1&vector=AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:X)

CVE-2024-40711

Es besteht eine Schwachstelle in Veeam Backup & Replication. Diese Sicherheitslücke wird derzeit nicht im Detail beschrieben. Ein entfernter, anonymer Angreifer kann diese Schwachstellen ausnutzen, um beliebigen Code auszuführen.

CVSS v3.1 Base Score: 10.0 / Temporal Score: 8.7
AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:X (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?version=3.1&vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:X)

Empfehlungen (1)

05.09.2024
Veeam stellt Updates zur Verfügung. Bitte installieren Sie die aktuelle Version unter Berücksichtigung Ihrer Betriebssystemumgebung.

https://www.veeam.com/kb4649 (https://www.veeam.com/kb4649)

Informationen (1)

05.09.2024
Veeam Security Bulletin September 2024 vom 2024-09-04

https://www.veeam.com/kb4649 (https://www.veeam.com/kb4649)

Referenzen (6)

CVE:CVE-2024-39718
CVE:CVE-2024-40710
CVE:CVE-2024-40711
CVE:CVE-2024-40712
CVE:CVE-2024-40713
CVE:CVE-2024-40714

Versionshistorie (1)

05.09.2024: Initiale Fassung