Multiple Vulnerabilities in Commvault Backup & Recovery Could Allo

Data: 2025-08-27 20:49:11

Autor: Inteligência Against Invaders

MS-ISAC ADVISORY NUMBER:

2025-074

DATE(S) ISSUED:

08/20/2025

OVERVIEW:

Multiple vulnerabilities have been discovered in Commvault Backup & Recovery, which when chained together, could allow for remote code execution. Commvault Backup & Recovery is a comprehensive data protection solution that offers a range of services for safeguarding data across various environments, including on-premises, cloud, and hybrid setups. Successful exploitation of these vulnerabilities could allow an attacker to bypass authentication, escalate privileges, run arbitrary commands, and potentially drop a JSP webshell.

THREAT INTELLIGENCE:

Researchers from watchTowr Labs have posted a detailed write-up about the vulnerabilities on their website.

SYSTEMS AFFECTED:

- Commvault versions 11.32.0 – 11.32.101 for Linux and Windows.
- Commvault versions 11.36.0 – 11.36.59 for Linux and Windows.

RISK:

Government:

Large and medium government entitiesHIGH

Small governmentMEDIUM

Businesses:

Large and medium business entitiesHIGH

Small business entitiesMEDIUM

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Commvault Backup & Recovery, which could allow for remote code execution.Details of the vulnerabilities are as follows:

Tactic: *Initial Access* (TA0001):

Technique: *Exploit Public-Facing Application* (T1190):

- A vulnerability in a known login mechanism allows unauthenticated attackers to execute API calls without requiring user credentials. RBAC helps limit the exposure but does not eliminate risk. (CVE-2025-57788)
- During the brief window between installation and the first administrator login, remote attackers may exploit the default credential to gain admin control. This is limited to the setup phase, before any jobs have been configured. (CVE-2025-57789)

- A security vulnerability has been identified that allows remote attackers to perform unauthorized file system access through a path traversal issue. The vulnerability may lead to remote code execution. (CVE-2025-57790)
- A security vulnerability has been identified that allows remote attackers to inject or manipulate command-line arguments passed to internal components due to insufficient input validation. Successful exploitation results in a valid user session for a low privilege role. (CVE-2025-57791)

The vulnerabilities can be exploited as part of two separate remote code execution (RCE) chains. One chain works only of the if the built-in admin password hasn't been changed since installation, and relies on exploiting CVE-2025-57788 (for bypassing authentication), CVE-2025-57789 (to escalate privileges), and CVE-2025-57790 to achieve RCE. The second chain, which works against any unpatched Commvault instance, uses CVE-2025-57791 to bypass authentication and CVE-2025-57790 for RCE (by injecting a webshell).

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by Commvault to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
- **Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
- **Safeguard 7.2: Establish and Maintain a Remediation Process:**Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
- **Safeguard 7.4: Perform Automated Application Patch Management:**Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- **Safeguard 7.5 : Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- **Safeguard 7.7: Remediate Detected Vulnerabilities:**Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:**Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
- **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:**Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the

enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

- **Safeguard 18.2: Perform Periodic External Penetration Tests:**Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
- **Safeguard 18.3: Remediate Penetration Test Findings:**Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
- **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:**Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
- **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts:**Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. (**M1016**:**Vulnerability Scanning**)
- **Safeguard 16.13: Conduct Application Penetration Testing:**Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

- Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems. (**M1030**:**Network Segmentation**)
- **Safeguard 12.2: Establish and Maintain a Secure Network Architecture:** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050:Exploit Protection**)
- **Safeguard 10.5:Enable Anti-Exploitation Features:**Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.