GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

1 September 2026

Advisory 217: Microsoft Azure Data Factory Multiple Vulnerabilities (CVE-2026-66800, CVE-2026-62834).

Release Date: 24th August 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations that use Microsoft Azure Data Factory for data integration or ETL pipelines. This alert is intended to be understood by technical users, cloud administrators and systems administrators.

What is it?

CVE-2026-66800 and CVE-2026-62834 are vulnerabilities in Microsoft Azure Data Factory, a cloud-based data integration service. CVE-2026-66800 is a server-side request forgery (SSRF) flaw that allows an unauthorized attacker to disclose information over the network. CVE-2026-62834 is a more severe flaw involving improper verification of a cryptographic signature, allowing an unauthorized attacker to elevate privileges over the network.

Both vulnerabilities can be triggered remotely without authentication or user interaction. Because Azure Data Factory is a Microsoft-managed platform-as-a-service, Microsoft addresses these vulnerabilities on the service side; however, organizations should still confirm through their Azure administration channels whether any tenant-side configuration review or action is expected for their environment.

What are the systems affected?

The following product is affected:

- Microsoft Azure Data Factory (all tenants) – (Affected by CVE-2026-66800 and CVE-2026-62834)

As a cloud service, Azure Data Factory does not have a customer-installed version number; Microsoft applies the service-side fix directly.

Organizations should monitor Microsoft's Security Update Guide entries for CVE-2026-66800 and CVE-2026-62834 and their Azure Service Health notifications for confirmation that the fix has been applied to their tenant, and for any recommended follow-up action.

What does this mean?

Typical attack flow:

1. **SSRF to information disclosure (CVE-2026-66800)**
    - An unauthenticated attacker sends a crafted request that causes Azure Data Factory to make an unintended server-side request, disclosing information the attacker should not have access to.
2. **Signature bypass to elevation of privilege (CVE-2026-62834)**
    - An unauthenticated attacker exploits improper cryptographic signature verification to have Azure Data Factory accept a forged or tampered request as legitimate, gaining elevated privileges over the network.

Attack vectors:

- Remote, unauthenticated network requests to the Azure Data Factory service (CVE-2026-66800 and CVE-2026-62834).
- No user interaction is required for either vulnerability.

Successful exploitation may allow attackers to:

- Disclose sensitive information reachable through Azure Data Factory's internal network requests.
- Elevate privileges within Azure Data Factory, potentially affecting data pipelines and connected resources.

Mitigation process

CERTVU recommends the following:

1. Confirm the Microsoft-side fix has been applied

- Check Microsoft's Security Update Guide entries for CVE-2026-66800 and CVE-2026-62834, and your organization's Azure Service Health notifications, for confirmation and any tenant-side guidance.

2. Review Data Factory access and network configuration
3. Restrict managed identities and connections

- Review linked services, managed identities and self-hosted integration runtime network access used by your Data Factory pipelines, and apply least privilege to each.

4. Audit pipeline activity logs

- Review Azure Monitor / Data Factory activity logs for unexpected outbound requests or privilege changes around the disclosure period.

5. Monitor Microsoft's security advisories page for further updates

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-66800
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62834