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

16 March 2026

Advisory 123: Ivanti Endpoint Manager (EPM) Authentication Bypass Vulnerability

Release Date: 09th March 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-1603 is a high-severity authentication bypass vulnerability affecting enterprise endpoint management software. The flaw exists in Ivanti Endpoint Manager (EPM) and allows a remote, unauthenticated attacker to bypass authentication controls and access sensitive stored credentials within the system.

The vulnerability results from improper authentication handling (CWE-288 / CWE-306) in the application. Specifically, certain internal API endpoints do not correctly enforce authentication checks, allowing attackers to access protected resources through alternative request paths.

What are the systems affected?

The vulnerability affects the following product and versions:

- **Ivanti Endpoint Manager**
- **All versions prior to 2024 SU5**, including:
  - 2024 base release
  - 2024 SU1
  - 2024 SU2
  - 2024 SU3
  - 2024 SU3 Security Release 1
  - 2024 SU4 and SU4 SR1

Endpoint Manager is widely used by organizations to:

- Manage enterprise endpoints (workstations and servers)
- Deploy software and security patches
- Manage credentials and administrative access

Because EPM typically operates with high administrative privileges across multiple endpoints, a compromise can potentially expose credentials used across the entire network.

What does this mean?

Attackers can exploit the vulnerability through the following process:

1. **Scanning for vulnerable systems**
   Attackers search the internet or internal networks for exposed Endpoint Manager servers.
2. **Sending crafted network requests**
   The attacker sends specially crafted HTTP requests targeting vulnerable internal API endpoints.
3. **Authentication bypass**
   Due to improper authentication checks in components such as WSAuth.dll, attackers can bypass session verification using techniques such as malformed headers or null-byte injection.
4. **Credential extraction**
   Once authentication is bypassed, attackers can access internal endpoints such as credential export APIs, allowing them to retrieve stored credential data.
5. **Post-exploitation activities**
   Stolen credentials may then be used to:
   - Gain administrative access to managed systems
   - Move laterally across the network
   - Deploy malware or ransomware
   - Compromise additional infrastructure

Because the attack requires no authentication and low complexity**,** it poses a significant threat to organizations using vulnerable versions

Mitigation process

CERTVU recommends the following:

- Apply Vendor Security Updates
- Restrict External Access
- Monitor for suspicious activity
- Implement security hardening

Reference

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.cve.org/CVERecord?id=CVE-2026-1603

.