

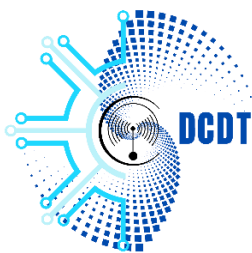
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

10 September 2026

Advisory 292: Dell Secure Connect Gateway Authentication Bypass, Command Execution, and Privilege Escalation Chain (CVE-2026-80172, CVE-2026-61410, and CVE-2026-80238).

Release Date: 9th September 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 and System/Network administrators that operate a Dell Secure Connect Gateway (SCG) 5.0 Appliance or Application. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-80172, CVE-2026-61410, and CVE-2026-80238 are three critical vulnerabilities in Dell Secure Connect Gateway (SCG) 5.0, Dell's remote-support connectivity platform used by organizations to allow Dell to remotely monitor and service their infrastructure. Dell is a major global enterprise IT vendor whose products, including SCG, are commonly deployed alongside Dell server and storage infrastructure (see also Advisory 234/278, Dell Power Store).

The three vulnerabilities form a documented escalation chain within the same certificate scope and remediation: CVE-2026-80172 allows an unauthenticated attacker to indefinitely replay a captured request to generate ADMIN access and refresh tokens, due to a lack of nonce validation or request time limits. CVE-2026-61410 is a missing-authorization flaw that permits an unauthenticated attacker to execute arbitrary commands via specially crafted requests, and CVE-2026-80238 allows a

low-privileged operator who already has SSH access to the SCG host to gain root-level access without a password, by abusing an exposed Docker socket.

What are the systems affected?

The following version(s) are affected:

- Dell Secure Connect Gateway 5.0 Appliance prior to version 5.36.00.16 - (Affected)
- Dell Secure Connect Gateway 5.0 Application prior to version 5.36.00.00 - (Affected)

Dell Secure Connect Gateway 5.0 Appliance 5.36.00.16 and later, and Application 5.36.00.00 and later - (Not affected, patched)

A single update to the fixed Appliance or Application version resolves all three vulnerabilities. There is no separate workaround for any of the three, so upgrading is the only remediation.

What does this mean?

Typical attack flow:

1. **Capture and replay a request to gain admin access**
 - An unauthenticated attacker captures a legitimate request to the SCG interface and, because there is no nonce validation or time limit on requests (CVE-2026-80172), replays it indefinitely to generate valid ADMIN access and refresh tokens.
2. **Execute commands remotely, then escalate to root on the host**
 - With admin-level access, the attacker sends specially crafted requests that exploit the missing-authorization flaw (CVE-2026-61410) to execute arbitrary commands on the system; if the attacker also has or obtains local SSH access, the exposed Docker socket flaw (CVE-2026-80238) then allows escalation to full, password-free root control of the underlying host.

Attack vectors:

- A network-based, unauthenticated attack against any reachable Dell SCG interface for the first two vulnerabilities (CVE-2026-80172 and CVE-2026-61410); the third (CVE-2026-80238) requires the attacker to already hold low-privileged local/SSH access to the SCG host.
- No user interaction is required for any of the three.

Successful exploitation may allow attackers to:

- Gain unauthenticated administrative access to the Dell SCG interface, and execute arbitrary commands on the underlying system.
- Escalate to full, password-free root-level control of the SCG host itself, and potentially use the remote-support connectivity platform's privileged position to reach the infrastructure it is meant to monitor and service.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Update Dell Secure Connect Gateway 5.0 Appliance to 5.36.00.16 or later, and Application to 5.36.00.00 or later, per Dell Security Advisory DSA-2026-382. A single update resolves all three vulnerabilities.

2. Restrict network access to the SCG management interface

3. Restrict and audit SSH access to the SCG host

4. Review access logs for signs of token replay or unauthorized admin activity

Report any suspected compromise of a Dell Secure Connect Gateway appliance or application to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-80172>
2. <https://www.cve.org/CVERecord?id=CVE-2026-61410>
3. <https://www.cve.org/CVERecord?id=CVE-2026-80238>
4. <https://www.dell.com/support/kbdoc/en-in/000503426/dsa-2026-382-security-update-for-dell-secure-connect-gateway-virtual-edition-multiple-vulnerabilities>