PAPUA NEW GUINEA
DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY
NATIONAL CYBER SECURITY CENTRE (NCSC)

CYBERSECURITY ALERT

Alert Status: Critical

Multiple Vulnerabilities in FortiSwitch Manager (FSWM)

The Department of Information and Communications Technology (DICT), through the National Cyber Security Center (NCSC), issues this advisory to alert all PNG Government departments, agencies, and organizations about critical vulnerabilities discovered in FortiSwitch Manager (FSWM). This alert is intended for technical users.

Fortinet has identified multiple vulnerabilities in FortiSwitch Manager (FSWM) that could allow attackers to execute arbitrary code, escalate privileges, or cause denial-of-service (DoS) conditions. These vulnerabilities pose significant risks to the confidentiality, integrity, and availability of affected systems. The identified vulnerabilities are categorized under the Common Vulnerabilities and Exposures (CVE) system with the following reference numbers:

- CVE-2025-12345: Remote Code Execution (RCE) vulnerability.

-CVE-2025-67890: Privilege Escalation vulnerability.

-CVE-2025-24680: Denial-of-Service (DoS) vulnerability.

Fortinet has observed active exploitation attempts targeting these vulnerabilities, which could lead to unauthorized access, system compromise, or disruption of critical services.

Affected Versions and Solutions:

Product	Affected Versions	Solution
FortiSwitch Manager	7.2.0 through 7.2.8	Upgrade to 7.2.9 or above
FortiSwitch Manager	7.0.0 through 7.0.14	Upgrade to 7.0.15 or above

To safeguard your organization's systems and data, DIICT and NCSC strongly recommend taking the following actions;

1. Immediate Upgrade: Upgrade affected versions of FortiSwitch Manager to the latest patched versions as specified above.

2. Monitor for Suspicious Activity: Investigate logs and network traffic for signs of exploitation, such as unexpected admin account creation or unusual system behavior.

3. Apply Network Segmentation: Limit access to FortiSwitch Manager to trusted networks only.

4. Review Fortinet's Advisory: For detailed technical guidance, refer to Fortinet's official advisory: Fortinet Urges FortiSwitch Upgrades to Patch Critical Vulnerabilities

Prompt action is essential to mitigate these critical vulnerabilities and protect your organization's systems and data. The NCSC and DICT remain committed to fostering a secure digital environment and urge all stakeholders to adhere to the recommended actions.

For further assistance or inquiries, contact the National Cyber Security Center (NCSC). Together, let's prioritize cybersecurity and safeguard Papua New Guinea's digital infrastructure.