Tuesday 5th November, 2024

CYBER ALERT

Alert Status: Critical

Fortinet FortiManager Missing Authentication Vulnerability

The Department of Information and Communications Technology (DICT) through the National Cyber Security Center (NCSC) issues alert to all IT Teams of PNG Government departments, agencies, and organizations about a critical vulnerability discovered in Fortinet FortiManager devices.

Fortinet, a prominent provider of security solutions like firewalls, endpoint security and intrusion detection systems, has issued an alert on October 23, 2024, of the existence of a critical function vulnerability in FortiManager fgfmd daemon. This vulnerability poses a significant risk as it could compromise the confidentiality, integrity, or availability of affected systems.

The identified vulnerability has a CVSS score of 9.8 and is categorized under the Common Vulnerabilities and Exposures (CVE) system with the following reference number: CVE-2024-47575. If successfully exploited, this vulnerability grants unauthorized control to the attacker to execute arbitrary code or commands via specially crafted requests.

Fortinet is aware of active exploitation of vulnerable instances. The vulnerable versions exploited in the wild are:

Version	Affected	Solution
FortiManager 7.6	7.6.0	Upgrade to 7.6.1 or above
FortiManager 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
FortiManager 7.2	7.2.0 through 7.2.7	Upgrade to 7.2.8 or above
FortiManager 7.0	7.0.0 through 7.0.12	Upgrade to 7.0.13 or above
FortiManager 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiManager 6.2	6.2.0 through 6.2.12	Upgrade to 6.2.13 or above
FortiManager Cloud 7.6	Not affected	Not Applicable
FortiManager Cloud 7.4	7.4.1 through 7.4.4	Upgrade to 7.4.5 or above
FortiManager Cloud 7.2	7.2.1 through 7.2.7	Upgrade to 7.2.8 or above
FortiManager Cloud 7.0	7.0.1 through 7.0.12	Upgrade to 7.0.13 or above
FortiManager Cloud 6.4	6.4 all versions	Migrate to a fixed release

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

1. All PNG Government departments, agencies, and organizations should check their networks for vulnerable FortiManager devices and follow the vendor's mitigation recommendations.
2. Patch information and mitigations are available. Users and Administrators are encouraged to see the Fortinet Advisory FG-IR-24-423.

Prompt action is crucial in addressing this critical vulnerability to ensure the security and stability of your organization's systems and data.

By remaining vigilant and keeping your infrastructure up-to-date, you can effectively safeguard against potential cyber threats. The NCSC and the Department of ICT are dedicated to promoting a secure digital environment, and we encourage all stakeholders to adhere to the recommended actions for enhanced cybersecurity resilience.

For any further assistance or inquiries, please reach out to the National Cyber Security Center (NCSC). Together, let us prioritize cybersecurity and protect Papua New Guinea's digital landscape.
Top of Form