JO-FinCERT – Security Advisory – 2023 – 47

1. Fortinet Fixes Critical FortiNAC Remote Command Execution Flaw

Fortinet released an update for its zero-trust access solution called FortiNAC. This update addresses a critical-severity vulnerability tracked as CVE-2023-33299, it could be exploited by attackers to execute malicious code and commands remotely.

The recently released update for FortiNAC aims to address a critical vulnerability, in order to prevent attackers from exploiting it to execute unauthorized code or commands within the network.

Recommendation:
It is essential for FortiNAC users to promptly apply the latest update to enhance the security of their network infrastructure.

CVE-2023-33299: Allows attacker to execute unauthorized code or commands via specifically crafted request on inter-server communication port. Note FortiNAC versions 8.x will not be fixed. CVSS (9.6/Critical)

Reference: https://www.fortiguard.com/psirt/FG-IR-23-074

2. Malware Delivery Exploit Found in Microsoft Teams Allows Attacks from External Sources

Researchers have recently discovered a technique that enables the delivery of malware through Microsoft Teams, bypassing the application's built-in restrictions on files from external sources.

The attack takes advantage of the default configuration in Microsoft Teams, which allows communication with external tenant accounts. The attack method is more powerful from social engineering and phishing attacks since it sending a malicious payload directly to a specific inbox, this will increase the impact of the attack.

Recommendations:
It is recommended for organizations that use Microsoft Teams and do not need to maintain regular communication with external tenants is to disable the External Access feature from "Microsoft Teams Admin Center > External Access."
If external channels of communication need to be maintained, organizations can define specific domains in an allow-list, to lower the risk of exploitation.

Reference:https://www.bleepingcomputer.com/news/security/microsoft-teams-bug-allows-malware-delivery-from-external-accounts/