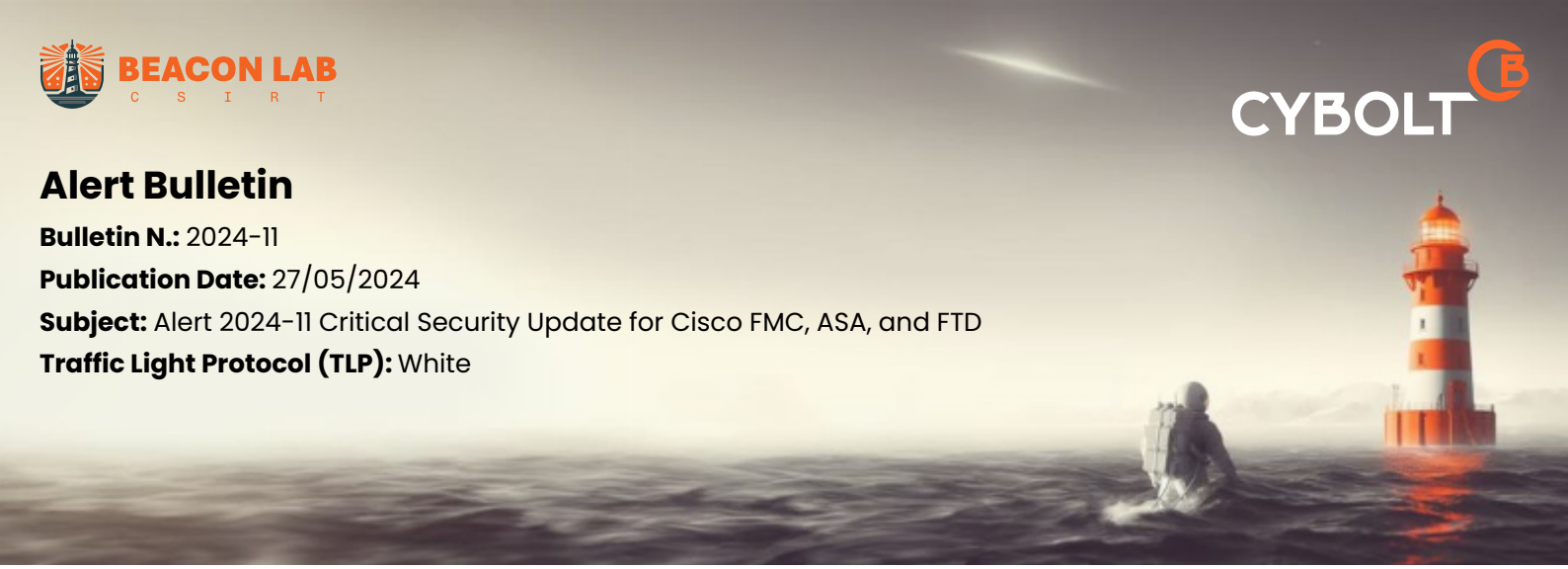

Alert Bulletin

Bulletin N.: 2024-11
Publication Date: 27/05/2024
Subject: Alert 2024-11 Critical Security Update for Cisco FMC, ASA, and FTD
Traffic Light Protocol (TLP): White

Affected Product(s):

- **Firepower Management Center (FMC)**
- **Cisco Adaptive Security Appliance (ASA)**
- **Cisco Firepower Threat Defense (FTD)**

Description:

Cisco has addressed a set of vulnerabilities identified as **CVE-2024-20355**, **CVE-2024-20363**, **CVE-2024-20261**, **CVE-2024-20361**, **CVE-2024-20293**, and **CVE-2024-20360**, with the latter being the most critical, having a severity score of **8.8**.

These vulnerabilities affect **Cisco ASA**, **FTD**, and **FMC** products. The most significant risk lies in the **FMC web management interface**, where an **SQL injection vulnerability** allows an attacker to manipulate SQL queries to obtain data from the database, execute commands on the host system, and escalate privileges. To exploit this vulnerability, an attacker must first possess the credentials of a user with read permissions on the management interface.

It is important to note that, as of today, there have been no recorded exploits of this vulnerability. The recently published patch mitigates this and the other mentioned vulnerabilities, including those involved in the attack campaign known as **ArcaneDoor**, which aimed to compromise Cisco ASA and FTD devices to implant malware, execute commands, and exfiltrate data from compromised devices.

Impact:

A malicious actor who has gained access to the network can exploit these vulnerabilities to manipulate the local database and execute malicious commands, gaining persistence on the machine hosting **FMC** and increasing their ability to attack the internal network.

Additionally, the previously mentioned medium-severity vulnerabilities are related to evading application rules or configurations, which could allow an attacker to bypass them.

Solution:

Apply the official patch published by Cisco.