Subject: **Cyber Security Advisory - Power Management Software Vulnerability in Data Centers (Advisory No. 51)**

Recently, **Trellix**[1] Advance Research Center has uncovered a number of vulnerabilities in **CyberPower's**[2] PowerPanel Enterprise, Data Center Infrastructure Management **(DCIM)**[3] platform and **Dataprobe's**[4] iBoot Power Distribution Unit (PDU). Details are given in ensuing paras:

2. **Summary of Vulnerabilities**

a. Following 4 x major vulnerabilities in CyberPower's PowerPanel Enterprise and 5 x critical vulnerabilities in the Dataprobe's iBoot PDU have been reported:

(1) **CyberPower's PowerPanel Enterprise**. CyberPower's PowerPanel Enterprise DCIM platform allows IT staff to manage, configure and monitor the infrastructure within a data center serving as a single source of information and control for all devices. The reported vulnerabilities are as follows:

(a) **CVE-2023-3264:** Use of hard-coded credentials (CVSS 6.7)

(b) **CVE-2023-3265:** Improper neutralization of escape, Meta or control sequences (Auth Bypass; CVSS 7.2)

(c) **CVE-2023-3266:** Improperly implemented security check for standard (Auth Bypass; CVSS 7.5)

(d) **CVE-2023-3267:** OS command injection (Authenticated RCE; CVSS 7.5)

(2) **Dataprobe iBoot PDU**

(a) **CVE-2023-3259:** Deserialization of untrusted data (Auth Bypass; CVSS 9.8)

(b) **CVE-2023-3260:** OS command injection (Authenticated RCE; CVSS 7.2)

(c) **CVE-2023-3261:** Buffer overflow (DOS; CVSS 7.5)

(d) **CVE-2023-3262:** Use of hard-coded credentials (CVSS 6.7)

---

[4] **Trellix** is a cyber security company, based in USA.

[2] **CyberPower** is a USA based company to design and manufacture a wide range of innovative power products, PDUs and Power management systems.

[3] **DCIM** tools monitors, measure, manage datacenter utilization and energy consumption.

[4] **Dataprobe** is an American manufacturer of system for minimizing downtime to critical data.

(e) **CVE-2023-3263:** Authentication bypass by alternate name (Auth Bypass; CVSS 7.5)

b. **Impact**. Following implications are foreseen after exploitation of the above-mentioned vulnerabilities by an attacker:

(1) By accessing power management system, attacker can control devices connected to a PDU and manipulate power management to damage the hardware devices.

(2) Unauthorized access to data center systems, thus allowing the attacker to switch off the power and infect data center to utilize compromised resources and further initiate attacks at large scale.

(3) Both products are vulnerable to remote code injection, thereby, attacker can install a backdoor and exploit system and devices.

3. **Recommendations**

a. PowerPanel Enterprise and Dataprobe iBoot PDU are recommended to be updated to the following versions:

(1) PowerPanel Enterprise software - **Version 2.6.9.**

(2) Dataprobe iBoot PDU firmware - **Version 1.44.08042023.**

b. Ensure PowerPanel Enterprise or iBoot PDU should be reachable only from organization’s secure intranet.

c. In case of the iBoot PDU, disable remote access via Dataprobe’s cloud service as an added precaution.