

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Data Center Vulnerabilities a Ticking Time Bomb for Cloud Services**

Date of Publication

August 22, 2023

Admiralty Code

A1

TA Number

TA2023340
















# Summary

**First Seen:** August 12, 2023

**Affected Product:** Dataprobe iBoot PDU, CyberPower PowerPanel Enterprise

**Impact:** Several flaws in critical data center infrastructure management systems and power distribution units pose a significant risk to cloud-based services. CyberPower's PowerPanel Enterprise has four vulnerabilities, and Dataprobe's iBoot PDU has five. When these flaws are exploited together, attackers could potentially acquire complete system access and administrator privileges, resulting in substantial risks. These include extensive malware deployment, espionage, and the possibility of power disruptions.

## CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-3264	Dataprobe authentication bypass Vulnerability	Dataprobe iBoot PDU			
CVE-2023-3265	CyberPower authentication bypass Vulnerability	CyberPower PowerPanel Enterprise			
CVE-2023-3266	CyberPower Improperly Implemented Security Check	CyberPower PowerPanel Enterprise			
CVE-2023-3267	CyberPower OS Command Injection Vulnerability	CyberPower PowerPanel Enterprise			
CVE-2023-3259	Dataprobe Deserialization of Untrusted Data	Dataprobe iBoot PDU			

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-3260	Dataprobe OS Command Injection Vulnerability	Dataprobe iBoot PDU	✗	✗	✓
CVE-2023-3261	CyberPower OS Command Injection Vulnerability	CyberPower PowerPanel Enterprise	✗	✗	✓
CVE-2023-3262	Dataprobe hard-coded credentials Vulnerability	Dataprobe iBoot PDU	✗	✗	✓
CVE-2023-3263	Dataprobe authentication bypass by alternate name	Dataprobe iBoot PDU	✗	✗	✓

# Vulnerability Details

## #1

Numerous vulnerabilities have been identified in data center infrastructure management systems and power distribution units, presenting a significant threat to widely-used cloud-based services. Specifically, there are four vulnerabilities in the CyberPower PowerPanel Enterprise Data Center Infrastructure Management (DCIM) platform and five critical vulnerabilities in the Dataprobe iBoot Power Distribution Unit (PDU). If exploited in a chained manner, these vulnerabilities could provide attackers with complete access to these systems, potentially resulting in significant harm.

## #2

The CyberPower PowerPanel Enterprise DCIM platform is a centralized cloud-based tool for IT teams to oversee, set up, and monitor data center infrastructure. On the other hand, the Dataprobe iBoot PDU facilitates remote management of power distribution to devices and equipment through a user-friendly web application. These platforms find common use across various deployment scales, ranging from on-premise servers to expansive co-located data centers. Notably, they are employed by major cloud providers like AWS, Google Cloud, and Microsoft Azure.

# #3

One of the vulnerabilities (CVE-2023-3265) enables unauthorized attackers to acquire administrator access to the CyberPower PowerPanel Enterprise by exploiting hardcoded default credentials. In contrast, the vulnerability associated with the Dataprobe iBoot PDU entails the utilization of hard-coded credentials to manipulate the internal Postgres database, potentially providing a malicious agent with the capability to alter database records.

# #4

Exploiting these vulnerabilities within data center setups could enable large-scale malware deployment, espionage, and even lead to power outages. The compromise of these platforms serves as a gateway for adversaries to infiltrate a significant number of systems and devices within data center environments.

## Vulnerability

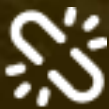
CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-3264	Dataprobe iBoot PDU version 1.43.03312023 or earlier	cpe:2.3:o:dataprobe:iboot-pdu4a-c10_firmware:*:*:*:*:*:*:*	CWE-798
CVE-2023-3265	CyberPower PowerPanel Enterprise earlier to Version 2.6.9	cpe:2.3:a:cyberpower:powerpanel_server:*:*:*:*:enterprise:*:*:*	CWE-150
CVE-2023-3266	CyberPower PowerPanel Enterprise earlier to Version 2.6.9	cpe:2.3:a:cyberpower:powerpanel_server:*:*:*:*:enterprise:*:*:*	CWE-358
CVE-2023-3267	CyberPower PowerPanel Enterprise server earlier to Version 2.6.9	cpe:2.3:a:cyberpower:powerpanel_server:*:*:*:*:enterprise:*:*:*	CWE-78
CVE-2023-3259	Dataprobe iBoot PDU version 1.43.03312023 or earlier	cpe:2.3:o:dataprobe:iboot-pdu4a-c10_firmware:*:*:*:*:*:*:*	CWE-502
CVE-2023-3260	CyberPower PowerPanel Enterprise server version 1.43.03312023 or earlier	cpe:2.3:a:cyberpower:powerpanel_server:*:*:*:*:enterprise:*:*:*	CWE-78
CVE-2023-3261	CyberPower PowerPanel Enterprise server earlier to Version 2.6.9	cpe:2.3:a:cyberpower:powerpanel_server:*:*:*:*:enterprise:*:*:*	CWE-78

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-3262	Dataprobe iBoot PDU running firmware version 1.43.03312023 or earlier	cpe:2.3:o:dataprobe:iboot-pdu4a-c10_firmware:*:*:*:*:*:*:*	CWE-798
CVE-2023-3263	Dataprobe iBoot PDU running firmware version 1.43.03312023 or earlier	cpe:2.3:o:dataprobe:iboot-pdu4a-c10_firmware:*:*:*:*:*:*:*	CWE-287 CWE-289

# Recommendations



**Apply Official Fixes Immediately:** Both Dataprobe and CyberPower have issued remedies for these vulnerabilities. Take swift action by upgrading to the latest software versions: PowerPanel Enterprise software version 2.6.9 and Dataprobe iBoot PDU firmware version 1.44.08042023. We strongly recommend that all potentially affected users promptly download and install these [patches](#) to effectively address the vulnerabilities.



**Strengthen Default Credential Management:** Take proactive measures to enhance default credential management practices. Conduct a thorough review and proceed to update default credentials, ensuring they are both unique and complex while maintaining secure storage. This proactive approach will effectively deter unauthorized access attempts and contribute to an overall fortified security stance for the systems.



**Implement Access Restrictions:** Ensure that both your PowerPanel Enterprise and iBoot PDU are inaccessible from the broader internet. Confine their accessibility exclusively to your organization's secure intranet. This practice effectively minimizes exposure to external threats. Additionally, for the Dataprobe iBoot PDU, contemplate the deactivation of remote access via Dataprobe's cloud service.



**Enforce strong access controls:** Implement strict access controls and authentication mechanisms. Utilize strong passwords, two-factor authentication, and role-based access control (RBAC) to ensure that only authorized personnel can access and make changes to the system.

# Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation
<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0006</u></b> Credential Access	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1133</u></b> External Remote Services
<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1040</u></b> Network Sniffing	<b><u>T1552</u></b> Unsecured Credentials	<b><u>T1078</u></b> Valid Accounts
<b><u>T1078.001</u></b> Default Accounts			

## Patch Details

CyberPower and Dataprobe have addressed these vulnerabilities through updates. The PowerPanel Enterprise software has been upgraded to version 2.6.9, while the Dataprobe iBoot PDU firmware now stands at its most recent version, 1.44.08042023.

Links:

[https://www.cyberpower.com/global/en/product/series/powerpanel\\_enterprise#downloads](https://www.cyberpower.com/global/en/product/series/powerpanel_enterprise#downloads)

<https://dataprobe.com/upgrade/iboot-pdu/iBoot-PDU-1.44.08042023.img>

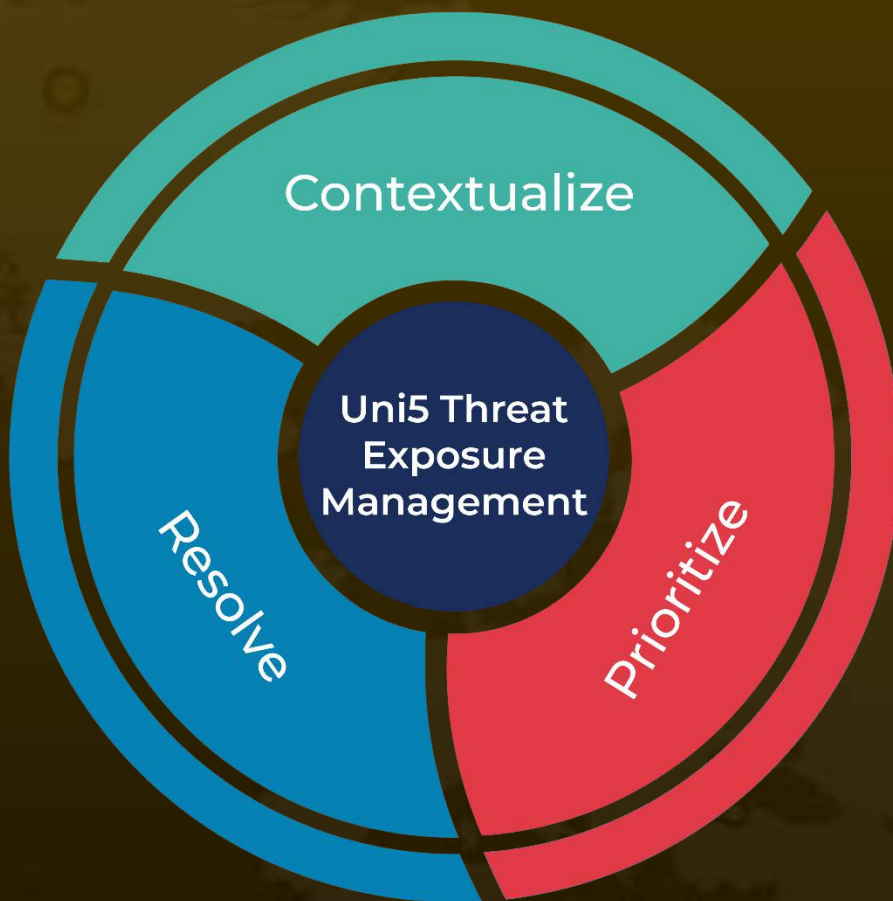
## References

<https://www.trellix.com/en-us/about/newsroom/stories/research/the-threat-lurking-in-data-centers.html>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**August 22, 2023 • 10:00 PM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)