

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Zero-Day Vulnerabilities in I-O Data Routers Expose Critical Security Risks

Date of Publication

December 6, 2024

Last Update Date

December 31, 2024

Admiralty Code

A1

TA Number

TA2024454










Summary

First Seen: December 2024

Affected Products: UD-LT1, UD-LT1/EX firmware

Impact: Hackers are exploiting zero-day vulnerabilities in I-O Data router devices, allowing them to change device settings, run unauthorized commands, and even disable firewalls. These vulnerabilities, identified as CVE-2024-45841, CVE-2024-47133, and CVE-2024-52564, affect the UD-LT1, a hybrid LTE router designed for flexible connectivity, as well as its industrial-grade version, the UD-LT1/EX. These flaws pose serious security risks, giving attackers the ability to take over devices, tamper with configurations, and weaken network defenses.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-45841	I-O DATA DEVICE UD-LT1/EX Incorrect Permission Assignment for Critical Resource Vulnerability	UD-LT1, UD-LT1/EX firmware			
CVE-2024-47133	I-O DATA DEVICE UD-LT1/EX OS Command Injection Vulnerability	UD-LT1, UD-LT1/EX firmware			
CVE-2024-52564	I-O DATA DEVICE UD-LT1/EX Inclusion of Undocumented Features Vulnerability	UD-LT1, UD-LT1/EX firmware			

Vulnerability Details

#1

Several zero-day vulnerabilities have been discovered in I-O Data router devices, exposing users to significant security threats. These flaws allow attackers to modify device settings, execute arbitrary commands, and disable firewall protections, potentially leaving networks vulnerable to further exploitation. Given I-O Data's prominence as a Japanese electronics manufacturer specializing in routers, NAS devices, and other consumer technology, these vulnerabilities present a notable risk to both individual users and organizations relying on these devices.

#2

CVE-2024-45841, stems from incorrect permission assignments for critical resources. An attacker exploiting this flaw, even with a guest account, can access specific files and retrieve sensitive credentials stored within. Another flaw, CVE-2024-47133, allows a remote attacker with administrative privileges to execute arbitrary operating system commands. This level of access could enable attackers to gain full control over the device, manipulate its configurations, or use it as a foothold for further attacks.

#3

Perhaps the most concerning vulnerability is CVE-2024-52564, which results from undocumented features in the device's firmware. Exploiting this flaw enables remote attackers to disable the router's firewall, execute OS-level commands, or alter critical device settings. To address these issues, I-O Data has released firmware version v2.1.9, which resolves CVE-2024-52564. Fixes for CVE-2024-45841 and CVE-2024-47133 are addresses in the version 2.2.0.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-45841	UD-LT1 firmware Ver.2.1.8 and earlier UD-LT1/EX firmware Ver.2.1.8 and earlier	cpe:2.3:h:i-o_data:ud-lt1:*:*:*:*:* cpe:2.3:h:i-o_data:ud-lt1_ex:*:*:*:*:*	CWE-732
CVE-2024-47133	UD-LT1 firmware Ver.2.1.8 and earlier UD-LT1/EX firmware Ver.2.1.8 and earlier		CWE-78
CVE-2024-52564	UD-LT1 firmware Ver.2.1.8 and earlier UD-LT1/EX firmware Ver.2.1.8 and earlier		CWE-1242

Recommendations



Update the Firmware: Users of UD-LT1 and UD-LT1/EX devices should immediately update to firmware version v2.1.9 to address the risks associated with CVE-2024-52564. Fixes for CVE-2024-45841 and CVE-2024-47133 are addresses in the version 2.2.0. This update mitigates the potential for attackers to disable firewalls, execute arbitrary commands, or modify device settings.



Limit Account Access: Restrict the use of guest and administrative accounts to trusted individuals. Ensure all accounts are secured with strong, unique passwords to reduce the likelihood of credential abuse.



Implement Network Monitoring: Use network monitoring tools to identify and respond to suspicious activities, particularly from administrative accounts. Detecting unauthorized access early can prevent further exploitation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation	TA0006 Credential Access
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation
T1556 Modify Authentication Process			

Patch Details

Update to the latest firmware version, UD-LT1 firmware Ver.2.1.9 and UD-LT1/EX firmware Ver.2.1.9 to address the risks associated with CVE-2024-52564. Fixes for CVE-2024-45841 and CVE-2024-47133 are addresses in the version 2.2.0.

Link: https://www.iodata.jp/support/information/2024/11_ud-lt1/

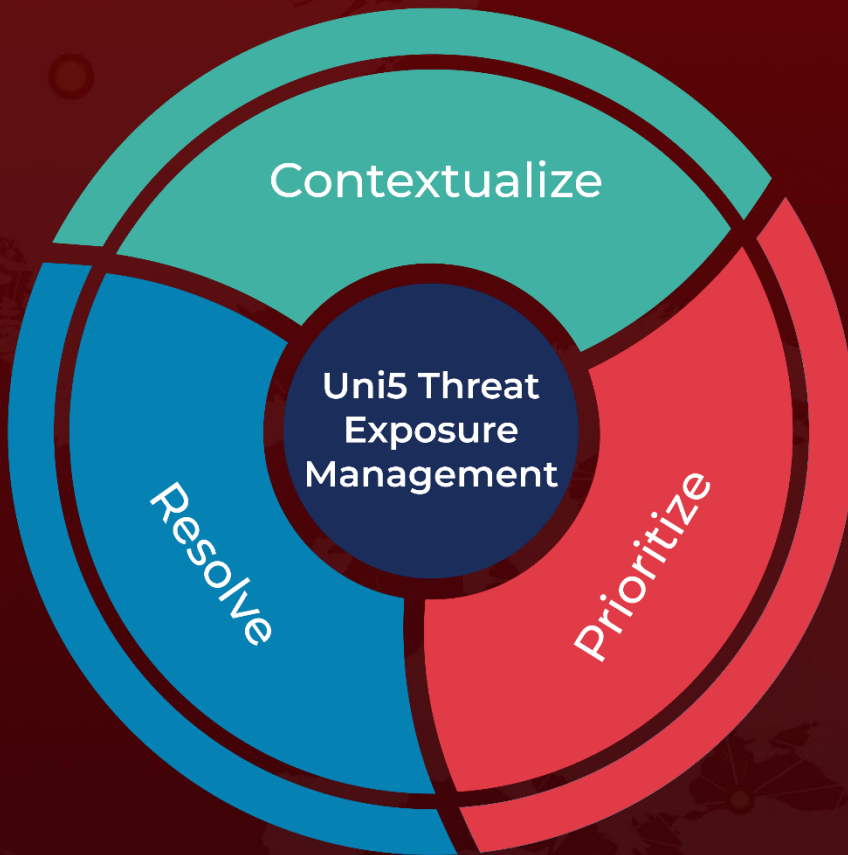
References

<https://jvn.jp/en/jp/JVN46615026/index.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

December 6, 2024 • 7:00 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com