

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

**Synology addresses the RCE vulnerability  
that affects VPN Plus servers**

Date of Publication

January 4, 2023

Admiralty Code

A1

TA Number

TA2023003


# Summary

**First Seen:** December 30, 2022

**Affected Product:** Synology VPN Plus Server

**Impact:** Execution of arbitrary commands leveraging unknown vectors.

## CVE

CVE	NAME	PATCH
CVE-2022-43931	Out-of-bounds write vulnerability in Synology	

# Vulnerability Details

Synology has addressed a flaw in VPN Plus Server that has the potential to take control affected systems. The vulnerability, identified as CVE-2022-43931, is an out-of-bounds write fault in Synology VPN Plus Server's remote desktop feature. When exploited, it allows remote attackers to execute arbitrary commands via undefined vectors, launch denial-of-service (DoS) attacks, and read arbitrary files.

## Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-43931	Synology VPN Plus Server before 1.4.3-0534 and 1.4.4-0635	cpe:2.3:a:synology:vpn_plus_server:*:*:*:*:*	CWE-787

# Recommendations



### Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.



### Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5’s Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the ‘Potential MITRE ATT&CK TTPs’ & ‘Patch Details’ on the following pages.

## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0003</u></b> Persistence	<b><u>TA0008</u></b> Lateral Movement
<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1543</u></b> Create or Modify System Process
<b><u>T1210</u></b> Exploitation of Remote Services			

## Patch Details

Upgrade to versions greater than 1.4.4-0635 and 1.4.3-0534.

[https://www.synology.com/en-global/security/advisory/Synology\\_SA\\_22\\_26](https://www.synology.com/en-global/security/advisory/Synology_SA_22_26)

## References

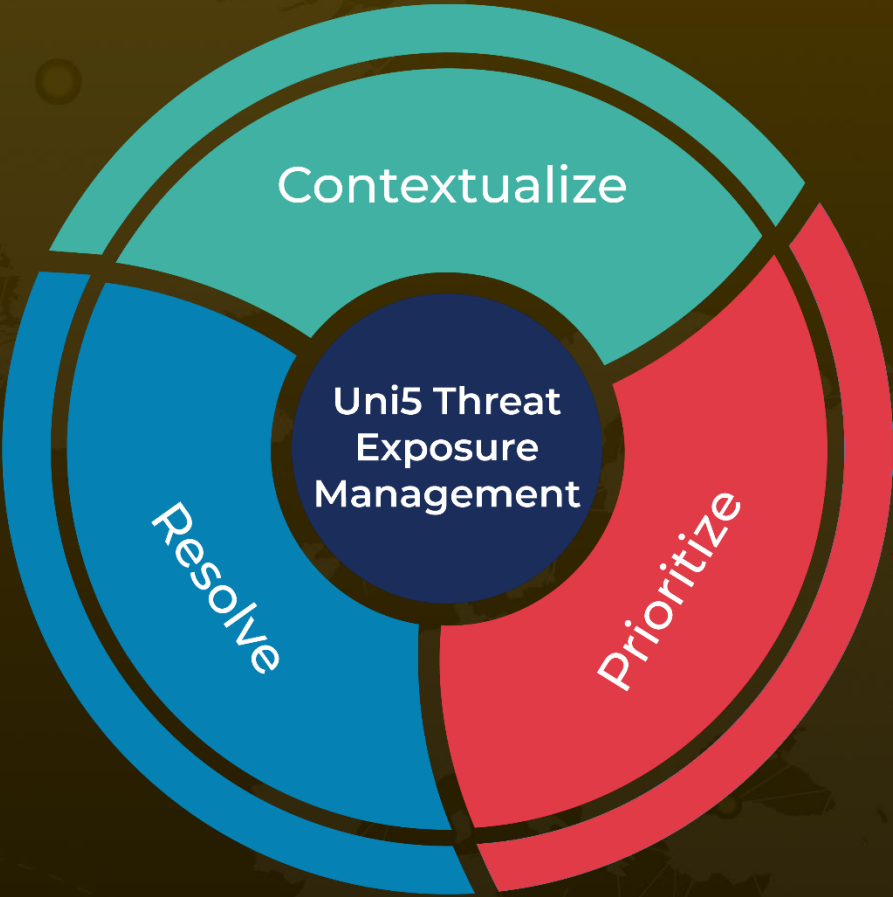
<https://www.bleepingcomputer.com/news/security/synology-fixes-maximum-severity-vulnerability-in-vpn-routers/>

[https://www.securityweek.com/critical-vulnerabilities-patched-synology-routers?&web\\_view=true](https://www.securityweek.com/critical-vulnerabilities-patched-synology-routers?&web_view=true)

# 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  
**January 4, 2023 • 2:00 AM**

© 2023 All Rights are Reserved by HivePro



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