Hive Pro

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

## Critical Zero-Day Exposes Synology Devices to Remote Attacks


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| November 12, 2025 | A1 | TA2025343 |

# Summary

**First Seen:** November 10, 2025
**Affected Products:** Synology BeeStation OS
**Impact:** A newly discovered zero-day vulnerability in Synology BeeStation OS has put users at serious risk, allowing attackers to remotely execute code and potentially take full control of affected devices. The flaw, caused by a buffer overflow issue, can be exploited without any user interaction, making it particularly dangerous. Synology has released an urgent patch for all versions from 1.0 to 1.3, and users are strongly advised to update immediately to secure their personal cloud devices and prevent possible exploitation.

## CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2025-12686 | Synology BeeStation OS Remote Code Execution Vulnerability | Synology BeeStation OS | ✓ | ✗ | ✓ |

# Vulnerability Details

**#1**

A critical zero-day vulnerability discovered in Synology BeeStation OS, which was successfully exploited at the Pwn2Own Ireland 2025 hacking competition, leaving devices exposed to potential remote code execution (RCE) attacks. BeeStation OS powers Synology's personal cloud storage devices, which include built-in applications like BeeFiles and BeePhotos for managing files and backing up photos, making it a valuable target for attackers seeking to compromise user data.

**#2** Tracked as CVE-2025-12686, the flaw stems from a “buffer copy without checking the size of input” error, which can be exploited to execute arbitrary code remotely. The issue originates from a buffer overflow vulnerability in the BeeStation OS, allowing unauthenticated attackers to run malicious code on the device without requiring any user interaction.

**#3** In simple terms, a buffer overflow occurs when a program writes more data into a memory buffer than it can handle, causing it to overwrite nearby memory regions. This flaw can be leveraged by threat actors to inject and execute harmful payloads, potentially granting them full control over the compromised device.

**#4** Synology has confirmed that BeeStation OS versions 1.0 through 1.3 are impacted by this vulnerability. The company has since released an updated version addressing the flaw. As no temporary mitigations are available, users are strongly advised to update their devices to the latest version immediately to safeguard against potential exploitation.

## Vulnerability

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2025-12686 | BeeStation OS 1.0, 1.1, 1.2, 1.3 | cpe:2.3:o:synology:beestation_os:*:*:*:*:*:*:*:* | CWE-120 |

# Recommendations

**Update Immediately:** Install the latest version of BeeStation OS released by Synology. This update includes a patch that fixes the vulnerability and is the only reliable way to stay protected.

**Disable Remote Access (If Not Needed):** Until you update, turn off any external or remote access features to reduce exposure to potential attacks.

**Use Strong Authentication:** Enable two-factor authentication (2FA) on your Synology account to add an extra layer of security against unauthorized logins.

**Monitor Device Activity:** Keep an eye on your BeeStation device for unusual behavior, such as unexpected reboots, slow performance, or unfamiliar files appearing. These may indicate compromise attempts.

**Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0042** Resource Development | **TA0001** Initial Access | **TA0002** Execution | **TA0004** Privilege Escalation |
| **T1190** Exploit Public-Facing Application | **T1068** Exploitation for Privilege Escalation | **T1059** Command and Scripting Interpreter | **T1588** Obtain Capabilities |
| **T1588.006** Vulnerabilities | | | |

## Patch Details

Update your BeeStation OS to the latest version.
BeeStation OS 1.3 - Upgrade to 1.3.2-65648 or above
BeeStation OS 1.2 - Upgrade to 1.3.2-65648 or above
BeeStation OS 1.1 - Upgrade to 1.3.2-65648 or above
BeeStation OS 1.0 - Upgrade to 1.3.2-65648 or above

Link: https://www.synology.com/en-global/security/advisory/Synology_SA_25_12

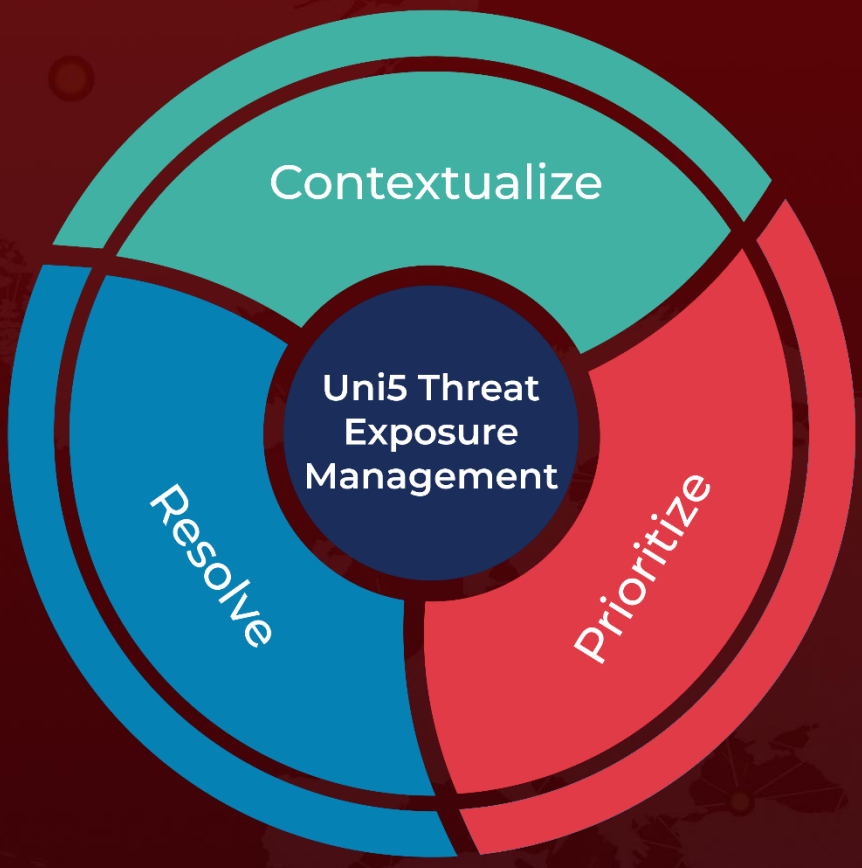
# References

https://www.synology.com/en-sg/security/advisory/Synology_SA_25_12

# 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

**November 12, 2025 . 7:30 AM**



More at www.hivepro.com