

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Patch Bypassed! Parallels Desktop Vulnerability Still Open to Attack**

Date of Publication

February 25, 2025

Admiralty Code

A1

TA Number

TA2025059




# Summary

**First Seen:** February 14, 2024

**Affected Product:** Parallels Desktop for Mac

**Impact:** CVE-2024-34331 is a critical vulnerability in Parallels Desktop for Mac, allowing attackers to gain root privileges by exploiting improper code signature verification of macOS installers. Although a patch was released in version 19.3.1, researchers found two bypass methods, making all known versions, including 20.2.1, vulnerable. Public exploits are available, posing serious security risks. Users are advised to implement precautionary measures and monitor for future updates from Parallels.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-34331	Parallels Desktop Privilege Escalation Vulnerability	Parallels Desktop for Mac			

# Vulnerability Details

## #1

CVE-2024-34331 is a critical security vulnerability affecting Parallels Desktop for Mac versions 19.3.0 and earlier. The vulnerability is due to improper verification of the code signature of macOS installers, allowing attackers to gain unauthorized root privileges.

## #2

This issue originates from the `repack_osx_install_app.sh` script, which uses the `createinstallmedia` tool to create macOS virtual machines without verifying its code signature. As a result, a malicious actor can replace the legitimate installer with a crafted, malicious version, gaining root access without requiring administrative authentication. This vulnerability was first discovered when researchers noticed that Parallels did not prompt for administrative credentials during macOS virtual machine creation.

## #3

Although Parallels released version 19.3.1 to address this issue by implementing code signature verification, recent findings revealed that the patch was insufficient. Security researchers disclosed two methods to bypass the patch. The first method involves a Time-of-Check to Time-of-Use (TOCTOU) attack, which exploits a race condition between the verification and execution of the `createinstallmedia` tool.

## #4

The second method leverages weak signature requirements, allowing malicious code to be injected into any Apple-signed binary, such as the system's `ls` command. These bypasses were responsibly disclosed in mid-2024 but were made public in February 2025 due to the absence of a response or a functional patch from Parallels.

## #5

The impact of this vulnerability is severe, as it allows attackers to execute arbitrary code with root privileges, compromising the underlying macOS host. This poses significant security risks for users who rely on Parallels Desktop for development, testing, and operational tasks. Notably, all known versions of Parallels Desktop, including version 20.2.1, are still vulnerable to these exploits.

## #6

Due to the public availability of these exploits, users are strongly advised to take precautionary measures, such as disabling automatic execution via `prl_disp_service`, auditing installer sources, and implementing endpoint detection solutions to monitor unauthorized system modifications. Until Parallels releases an effective patch, users should remain vigilant and consider limiting or suspending the use of Parallels Desktop in high-security environments.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-34331	Parallels Desktop: All versions	<code>cpe:2.3:a:parallels:desktop:19.0:*:*:*:*:*</code>	CWE-269

# Recommendations



**Update and Patch Management:** Continuously monitor for updates from Parallels and apply security patches as soon as they are released. Although the current patch (version 19.3.1) is insufficient, staying up-to-date minimizes exposure to known vulnerabilities.



**Restrict Privileges:** Disable automatic execution of Parallels Desktop's `prl_disp_service` using macOS Privacy Controls under System Settings > Security > Automation. This prevents unauthorized code execution.



**Source Verification and Auditing:** Only use macOS installer images obtained directly from verified Apple distribution channels. Regularly audit downloaded installers to ensure integrity and authenticity.



**Endpoint Detection and Monitoring:** Implement endpoint detection solutions to monitor and alert on unexpected modifications in critical system directories, especially in `/Library/` and Parallels' resource directories.



**Verify Code Signatures:** Enforce strict code signature verification for all software installations to prevent the execution of unverified or malicious installers. Use macOS tools and system integrity protection to ensure only trusted code runs.



## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0002</u></b> Execution	<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0005</u></b> Defense Evasion
<b><u>T1588.005</u></b> Exploits	<b><u>T1553.002</u></b> Code Signing	<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1553</u></b> Subvert Trust Controls
<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1588</u></b> Obtain Capabilities	

## Patch Details

Parallels released version 19.3.1 to address this vulnerability by implementing code signature verification for the createinstallmedia binary. However, the patch has been proven insufficient due to the two new exploitation methods. Parallels has yet to release an effective update that mitigates these bypasses.

Links:

<https://www.parallels.com/products/desktop/download/>

<https://kb.parallels.com/129860>

## References

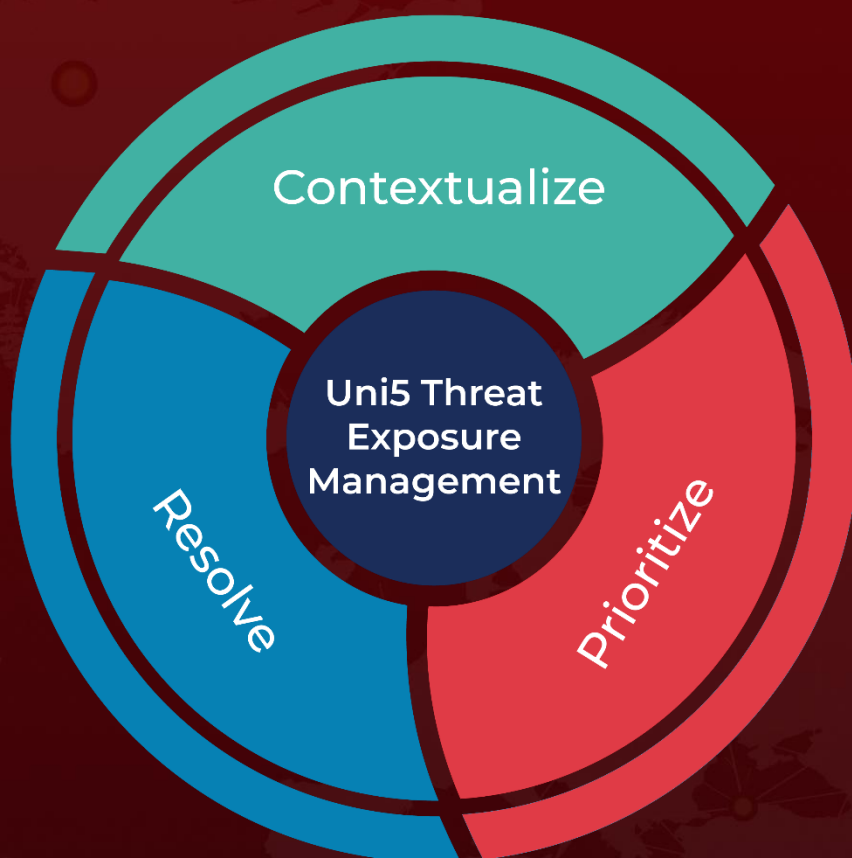
<https://jhftss.github.io/Parallels-0-day/>

<https://kchronokernel.com/macOS/2024/05/30/CVE-2024-34331.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

**February 25, 2025 • 9:30 AM**

© 2025 All Rights are Reserved by Hive Pro



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