

## OMSA-2025-0001: Horizon Client for Windows addresses local privilege escalation vulnerability (CVE-2025-25230)

Advisory ID: OMSA-2025-0001

Severity: High

CVSSv3 Range: 7.8

Issue Date: 2025-04-16

Updated On: 2025-04-16 (Initial Advisory)

CVE(s): CVE-2025-25230

---

### 1. Impacted Products

- Omnissa Horizon Client for Windows

### 2. Introduction

A local privilege escalation (LPE) vulnerability was privately reported in Omnissa Horizon Client for Windows. Updates are available to remediate this vulnerability in impacted versions of the client.

### 3. Advisory Details

#### Description

Omnissa Horizon Client for Windows contains an LPE Vulnerability. Omnissa has evaluated the severity of this issue to be in the High severity range with a maximum CVSSv3 base score of [7.8](#).

#### Known Attack Vectors

A malicious actor with local access where Horizon Client for Windows is installed may be able to elevate privileges.

## Resolution

To remediate CVE-2025-25230, apply the patches listed in the 'Fixed Version' column of the 'Resolution Matrix' found below.

## Acknowledgements

Omnissa would like to thank Bocheng Xiang (@Crispr) From FDU for reporting this issue to us.

## Resolution Matrix

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
Horizon Client for Windows	Any	Windows	CVE-2025-25230	<a href="#">7.8</a>	High	<a href="#">2503</a>	None	None
Horizon Client for macOS	Any	macOS	CVE-2025-25230	n/a	Not Impacted	Not Impacted	n/a	n/a
Horizon Client for Linux	Any	Linux	CVE-2025-25230	n/a	Not Impacted	Not Impacted	n/a	n/a
Horizon Client for iOS	Any	iOS	CVE-2025-25230	n/a	Not Impacted	Not Impacted	n/a	n/a
Horizon Client for Android	Any	Android	CVE-2025-25230	n/a	Not Impacted	Not Impacted	n/a	n/a
Horizon Client for Chrome	Any	Chrome	CVE-2025-25230	n/a	Not Impacted	Not Impacted	n/a	n/a

## 4. References

Downloads and Documentation:

Omnissa Horizon Client for Windows Release Notes  
<https://docs.omnissa.com/bundle/horizon-client-windows-RNV2503/page/HorizonClientWindows-ReleaseNotes.html>

Omnissa Horizon Client for Windows 2503  
[https://customerconnect.omnissa.com/downloads/details?downloadGroup=CART26FQ1\\_WIN\\_2503&productId=1562&rPId=118986](https://customerconnect.omnissa.com/downloads/details?downloadGroup=CART26FQ1_WIN_2503&productId=1562&rPId=118986)

Mitre CVE Dictionary Links:  
<https://nvd.nist.gov/vuln/detail/CVE-2025-25230>

FIRST CVSSv3 Calculator:

<https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H>

## 5. Change Log

2025-04-16: OMSA-2025-0001  
Initial security advisory

## 6. Contact

E-mail: [security@omnissa.com](mailto:security@omnissa.com)

Omnissa Security Advisories  
<https://www.omnissa.com/omnissa-security-response/>

Omnissa Security Response Policy  
<https://www.omnissa.com/omnissa-external-vulnerability-response-and-remediation-policy/>

Omnissa Product Lifecycle Matrix  
<https://docs.omnissa.com/bundle/Product-Lifecycle-Matrix/page/lifecyclematrix.html>

Copyright 2025 Omnissa, LLC. All rights reserved.