CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

Wednesday, November 26, 2025 **CAL-CSIC-202511-A-011**

Azure Bastion Privilege Escalation Vulnerability

Token | Virtual Machine | Azure Bastion | Bypass Authentication

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical authentication bypass vulnerability in Microsoft Azure Bastion. Azure Bastion is a managed Microsoft service that provides secure Remote Desktop Protocol (RDP) and Secure Shell (SSH) connectivity to virtual machines(VM) in Azure without exposing the VMs directly to the internet.[1] CVE-2025-49752, with a a CVSS v3.1 score of 10, allows remote attackers to bypass authentication mechanisms and escalate privileges to administrative levels.[2]

Affected Systems and Versions

- Product: Microsoft Azure Bastion
- Affected: All Azure Bastion deployments prior to the security update released on November 20, 2025
- No specific version numbers or SKU restrictions have been published in available advisories
- All configurations using Azure Bastion for RDP or SSH access are potentially affected

When exploited, attackers can intercept and replay valid authentication tokens to gain unauthorized administrative access to all virtual machines connected through the affected Bastion host. The attack requires only a single network request and operates without user interaction.[3]

The Cal-CSIC recommends following Microsoft's guidance on mitigating this vulnerability.

For more information on CVE-2025-49752, please refer to Microsoft Security Response Center (MSRC) Update Guide.[4]

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

References

[1] Zero Path; "Azure Bastion CVE-2025-49752: Brief Summary of Critical Elevation of Privilege Vulnerability"; https://zeropath.com/blog/azure-bastion-cve-2025-49752; accessed 24 November 2025
[2] NVD; "CVE-2025-49752 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2025-49752; accessed 24 November 2025
[3] Cyber Press; "Attackers Bypass Authentication and Escalate Privileges via Critical Azure Bastion Vulnerability"; https://cyberpress.org/azure-bastion-vulnerability/; accessed 24 November 2025
[4] MSRC; "Azure Bastion Elevation of Privilege Vulnerability"; https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49752; accessed 24 November 2025

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.