Smarttech
YOUR 24/7 SECURITY PARTNER

Critical Vulnerabilities in VMware Workstation and Fusion – 3rd September 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	150
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-03
Issue Date	2026-09-03

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

New critical vulnerabilities were discovered in VMware Workstation and Fusion. Successful exploitation of these vulnerabilities could result in code execution on the host system.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

More details related to these vulnerabilities are as follows:

CVE ID	Description	Known Attack Vectors
CVE-2026-59346 **CVSS Base Score: 9.3**	VMware Workstation and Fusion contain an integer-overflow vulnerability.	A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host.
CVE-2026-59347 **CVSS Base Score: 8.1**	VMware Workstation and Fusion contain a stack-based buffer-overflow vulnerability in HGFS.	A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.

Affected Products

- VMware Workstation
- VMware Fusion

Response Matrix

Product	Version	Running On	CVE	CVSSv3	Severity	Fixed Version
VMware Workstation	25H2, 26H1	Any	CVE-2026-59346, CVE-2026-59347	9.3, 8.1	Critical	26H1u1
VMware Fusion	25H2, 26H1	MacOS	CVE-2026-59346, CVE-2026-59347	9.3, 8.1	Critical	26H1u1

Recommendations

Smarttech247 team recommend the following actions be taken:

- Upgrade VMware to the fixed version.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- **Use** the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

References

Support Content Notification - Support Portal - Broadcom support portal

CVE

CVE-2026-59346
CVE-2026-59347


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com