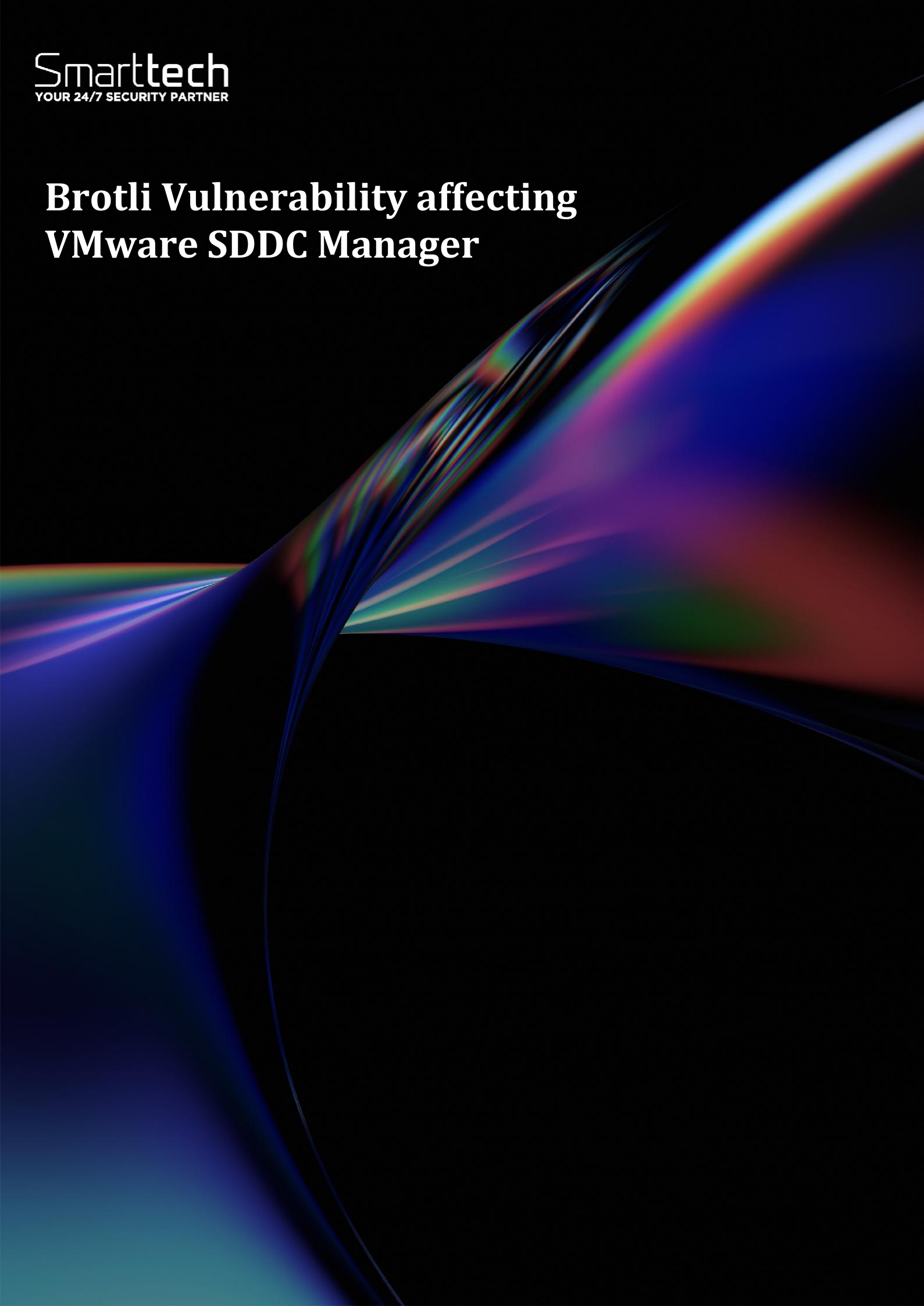


Brotli Vulnerability affecting VMware SDDC Manager



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	187
Authors	Daniel-Cristian Carp < daniel.carp@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-28
Issue Date	2026-10-28

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

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:

A critical out-of-bounds write vulnerability in the Google Brotli decoder, tracked as CVE-2026-111497, affects Node.js used by VMware SDDC Manager. A remote attacker with network access to SDDC Manager may exploit this vulnerability to execute arbitrary code.

RISK:

Government:

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

Businesses:

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

SYSTEMS AFFECTED:

The Broadcom advisory identifies the following affected products and SDDC Manager versions:

VMware Product	Component	Version	CVSSv3	Severity	Workarounds
VMware Cloud Foundation, VMware vSphere Foundation	SDDC Manager	9.1.1	9.8	Critical	KB460732
VMware Cloud Foundation, VMware vSphere Foundation	SDDC Manager	9.0.x, 9.1.0	7.5	Important	KB460734
VMware Cloud Foundation	SDDC Manager	5.2.x	7.5	Important	KB460734

Affected deployment scope: The affected products running on any platform. Exposure requires network access to SDDC Manager.

TECHNICAL SUMMARY:

CVE-2026-111497 (CWE-787: Out-of-bounds Write; CWE-252: Unchecked Return Value): Brotli decoder block-switch handling

The vulnerability occurs when the Brotli decoder mishandles invalid block-type switches, potentially causing writes beyond an eight-byte internal buffer and memory corruption. Under suitable conditions, an attacker supplying crafted compressed data may achieve remote code execution. The upstream fix introduces a dedicated format-error code to reject invalid block switches.

Recommendations:

Identify vulnerable systems and applications

- Identify VMware Cloud Foundation and VMware vSphere Foundation deployments running affected SDDC Manager versions: 9.1.1.x, 9.1.0, 9.0.x and VMware Cloud Foundation 5.2.x.
- Verify exact SDDC Manager versions and determine which Broadcom workaround applies to each deployment.
- Assess network exposure of SDDC Manager management interfaces, particularly access from untrusted networks.

Apply vendor remediation

- Apply the Broadcom-supported permanent fix as soon as it becomes available and verify remediation

Implement temporary mitigations

- Follow KB460732 for affected SDDC Manager 9.1.1.x deployments.
- Follow KB460734 for the applicable older releases documented by Broadcom.
- Restrict management-plane access to authorised administrative networks and trusted hosts.
- Back up relevant configurations and follow the vendor's instructions when implementing workarounds

Monitor for potential exploitation

- Review available firewall, application and system logs for suspicious requests and unexpected access to SDDC Manager.
- Investigate unexplained service crashes, restarts, abnormal processes and unexpected outbound network connections.
- Preserve relevant logs and correlate network and endpoint telemetry when investigating suspected compromise.

Strengthen infrastructure security

- Restrict SDDC Manager access to authorized administrators and trusted networks.
- Isolate management interfaces from internet-facing systems.
- Verify service functionality after applying workarounds or patches.
- Track affected VMware versions and Broadcom security updates.

References:

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/39445>

CVEs

CVE-2026-111497

