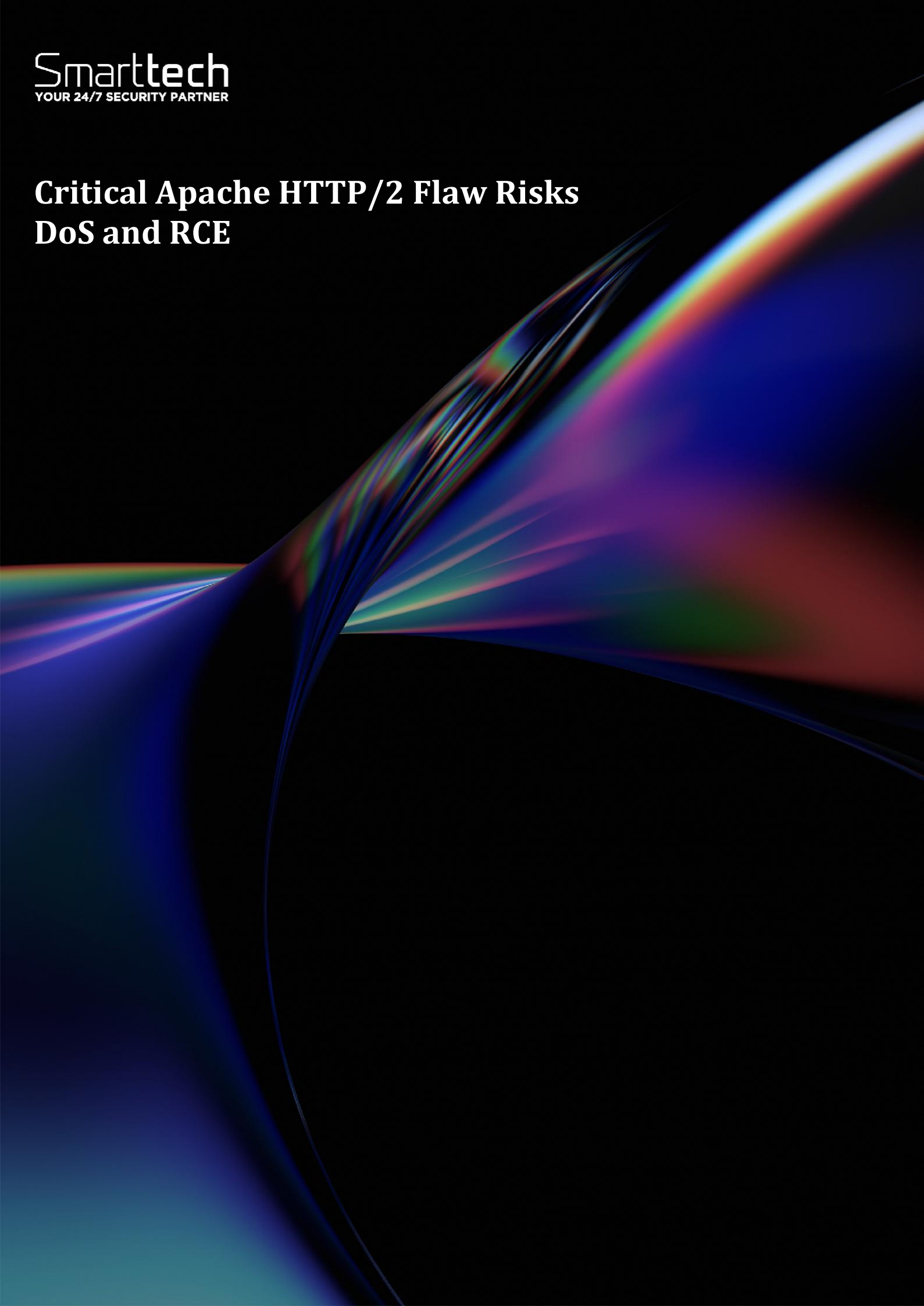
Smarttech
YOUR 24/7 SECURITY PARTNER

Critical Apache HTTP/2 Flaw Risks DoS and RCE



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	63
Authors	Maria-Iasmina Macovei < maria.macovei@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-05-06
Issue Date	2026-05-06

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 vulnerability has been disclosed in the Apache HTTP Server, affecting the HTTP/2 module (mod_http2) and posing a significant risk to exposed web services. Tracked as CVE-2026-23918, the flaw is caused by a double-free memory corruption issue in the HTTP/2 stream handling logic. It can be triggered by a remote, unauthenticated attacker through specially crafted HTTP/2 requests. The vulnerability affects Apache HTTP Server 2.4.66 and may result in denial-of-service (DoS) conditions by crashing the affected process. Under specific memory allocation conditions, it may also be leveraged to achieve remote code execution (RCE) within the context of the web server, potentially leading to full system compromise. Given the widespread deployment of Apache HTTP Server in internet-facing environments and the common use of HTTP/2 in default configurations, the attack surface is significant. Administrators are strongly advised to upgrade to Apache HTTP Server 2.4.67, which resolves this issue. As temporary mitigation, disabling the HTTP/2 module (mod_http2) and restricting external access to affected services can reduce exposure until patching is applied.

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 this vulnerability are as follows:

CVE ID	Description
CVE-2026-23918 **CVSS Base Score: 8.8**	Double Free and possible RCE vulnerability in Apache HTTP Server with the HTTP/2 protocol. This issue affects Apache HTTP Server: 2.4.66. Users are recommended to upgrade to version 2.4.67, which fixes the issue.

Affected Products

Product	Affected Version
Apache HTTP Server	2.4.66

Recommendations

Smarttech247 team recommend the following actions be taken:

- Upgrade Apache HTTP Server to version 2.4.67
- 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 endpoints, 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

https://httpd.apache.org/security/vulnerabilities_24.html

CVE

CVE-2026-23918

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com