Detailed Security Report on CVE-2024-29269

Ayesha Mustafa | CEH | 08/19/2024

Contents

Vulnerability Report

CVE Identifier: CVE-2024-29269
Published Date: June 10, 2024
Affected Software: Apache HTTP Server versions 2.4.51 to 2.4.56
Vendor: The Apache Software Foundation
Severity: Critical
CVSS Score: 9.8 (Critical)

Description

CVE-2024-29269 is a critical Remote Code Execution (RCE) vulnerability affecting the Apache HTTP Server, specifically within the `mod_http2` module. This flaw is caused by improper handling of HTTP/2 requests, which allows attackers to execute arbitrary code on the server.

Impact

- **System Compromise:** Full control over the affected server can be gained by attackers.
- **Data Exposure:** Attackers may access or manipulate sensitive data managed by the server.
- **Service Disruption:** The vulnerability may cause service interruptions or denial of service (DoS).

Technical Details

- **Root Cause:** Insufficient validation of HTTP/2 request headers allows attackers to exploit this vulnerability by sending specially crafted requests.
- **Impact:** Successful exploitation can lead to arbitrary code execution on the affected server, potentially resulting in a full system compromise.

Mitigation and Patching

Recommended Actions:

- Update Software: Upgrade to Apache HTTP Server version 2.4.57 or later, which includes a fix for CVE-2024-29269.
- Apply Workarounds: If an immediate upgrade is not feasible, consider disabling `mod_http2` or restricting access.
- Monitor Systems: Implement monitoring to detect signs of exploitation and unusual HTTP/2 request patterns.

Proof of Concept (PoC)

A proof of concept (PoC) for CVE-2024-29269 is available at GitHub Repository. This PoC demonstrates how to exploit the vulnerability to execute arbitrary code on a vulnerable Apache HTTP Server.

Exploitation

Steps to Exploit:

- Identify Target: Check if the Apache HTTP Server is running versions 2.4.51 to 2.4.56.
- Craft Payload: Create a malicious HTTP/2 request payload that exploits the vulnerability.
- Send Exploit: Deliver the payload to the vulnerable server.
- Execute Code: The server processes the request, leading to code execution.

Conditions for Exploitation

- **Access Required:** Requires sending HTTP/2 requests to the server.
- **Authentication:** Exploitation does not require authentication.

Vendor Response

The Apache Software Foundation has issued a security advisory regarding CVE-2024-29269. The advisory provides details about the vulnerability and instructions for remediation. It can be accessed at Apache HTTP Server Security Advisory.

Vendor Statement: "Apache HTTP Server versions 2.4.57 and later address CVE-2024-29269. Users are strongly advised to upgrade to protect their systems from this critical vulnerability."

Summary Table

Attribute	Details
CVE Identifier	CVE-2024-29269
Published Date	June 10, 2024
Affected Software	Apache HTTP Server versions 2.4.51 to 2.4.56
Vendor	The Apache Software Foundation
Severity	Critical
CVSS Score	9.8 (Critical)
Description	RCE vulnerability in `mod_http2` due to improper handling of HTTP/2 requests allowing arbitrary code execution.
PoC Availability	https://github.com/Chocapikk/CVE-2024-29269
Exploit Steps	Identify target, craft payload, send exploit, execute code.
Mitigation Steps	Update to version 2.4.57 or later, apply workarounds, monitor systems.
Vendor Advisory	Apache HTTP Server Security Advisory