National Cyber Security Centre

2110081008-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Apache HTTP Server 2.4.49/50 Vulnerabilities
2021-10-08

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

The NCSC would like to advise constituents of a vulnerability associated with Apache HTTP Server versions 2.4.49 and 2.4.50 (CVE-2021-41773,CVE-2021-42013) that is being actively scanned for by threat actors with an expectation that this will lead to exploitation.

The initial vulnerability in version 2.4.49 allowed a malicious actor to gain access to files outside of the root directory of the web server by executing a Path Traversal attack. Path Traversal attacks allow an attacker to send requests for files that would otherwise not be exposed to the Internet and access these files without authentication if certain protections have not been applied.

The initial vulnerability only affected servers running version 2.4.49. Earlier Apache Server versions were not vulnerable to CVE-2021-41773. Apache released a patch on October 5th to address CVE-2021-41773 however this patch was reported as incomplete and a subsequent complete patch to address CVE-2021-42013 was released on October 7th [1].

Products Affected

Apache HTTP Server 2.4.49
Apache HTTP Server 2.4.50

Impact

- Exfiltration of data
- Denial of service
- Remote Code Execution (under certain conditions)

Recommendations

The NCSC recommends that all organisations review their estate for Apache HTTP Server version 2.4.49, 2.4.50 and update to version 2.4.51 immediately to address the current issues.

[1] https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2021-42013

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie