UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00209

APACHE HTTP SERVER PATH TRAVERSAL ATTACKS

DATE ISSUED: 11th October 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Apache HTTP Server is a popular open-source, cross-platform web server for both Windows and Unix and those who use it should patch immediately, as this vulnerability is being actively exploited in the wild. Leaving the vulnerability open could allow for an attacker to perform a path traversal attack.

BREAKDOWN

Changes made to path normalisation in Apache HTTP Server version 2.4.49 allow for the execution of a path traversal attack where URLs are mapped to files outside the expected document root. Attackers send requests to access backend server directories, which are considered sensitive and should not be accessible. If the files within the directory are not then protected by "require all denied" access control which by default is disabled, such requests can succeed. Filters are able to be bypassed with encoded ASCII character for the URLs which once mapped can provide access to the root on the we server. Additionally the CGI scripts of the interpreted files may also be leaked during the process.

REMEDIATION STEPS

- Apply the latest Apache HTTP Server patch to bring the system up to version 2.4.50
- Ensure all software is run as non-privileged users to reduce the potential scale of a successful attack
- Educate users on the dangers of visiting untrusted websites.
- Apply the principle of least privilege across all systems and services running in your environment

REFERENCES & RESOURCES

CIS Advisory
Bleeping Computer https://www.bleepingcomputer.com/news/security/apache-fixes-actively-exploited-zero-day-vulnerability-patch-now/
Apache https://httpd.apache.org/security/vulnerabilities_24.html