**Pakistan Telecom Authority Headquarters, Islamabad**

**PTA Cyber Security Advisory No. 278** **14-06-2024**

**Name:** New PHP Vulnerability Exposes Windows Servers

**Threat Classification:** Vulnerability

**Affected Software / Services:**

- PHP 8.3 before 8.3.8
- PHP 8.2 before 8.2.20
- PHP 8.1 before 8.1.29

**Summary:**

A recently discovered critical security loophole in PHP has the potential to enable remote code execution in specific situations. Identified as CVE-2024-4577, this vulnerability, categorized as CGI argument injection, affects multiple PHP versions on Windows OS installations. It permits unauthorized individuals to sidestep the previously mitigated CVE-2012-1823 using certain character sequences. This oversight exposes remote PHP servers to the risk of executing arbitrary code through the injection attack.

| | |
|---|---|
| **Severity** | **Critical** |
| **Attack Vector** | Remote Code Execution |

**Recommendations:**

- It is strongly recommended that all users upgrade to the latest PHP versions. Link is attached below:

https://www.php.net/downloads.php

- It is recommended to evaluate the possibility of migrating to a more secure architecture such as Mod-PHP, Fast CGI, or PHP-FP.
- Keep all the systems and software's up to date with the latest security patches to prevent attackers from exploiting known vulnerabilities.
- In case of any incident, please report to this office, through PTA CERT Portal and email.