Memorandum

To: MotoCorp

From: Team 13

Subject: Web Vulnerabilities and Mitigations Assessment Report | WBV104

Date: 09/27/2024

Team 13 provides a brief report of 3 major vulnerabilities in our services.

(1) **Name**: HTTP.sys Remote Code Execution Vulnerability, aka CVE-2015-1635
   a. **Description**: a critical vulnerability that allows remote attackers to execute code through crafted HTTP web server requests to our affected systems.
   b. **Impact**: remote attackers could crash the site, causing downtime, and potentially execute code with elevated privileges.
   c. **Actions/Measures**: according to Microsoft Documentation, there are no mitigating factors for this vulnerability. However, a system update will resolve the vulnerability.

(2) **Name**: Elasticsearch Dynamic Script Arbitrary Java Execution, aka CVE-2014-3120
   a. **Description**: a critical vulnerability that allows remote attackers to execute code through the `to_search` parameter due to lack of authentication.
   b. **Impact**: remote attackers could compromise the server and gain access to sensitive information.
   c. **Actions/Measures**: the Logstash 1.4.3 update will resolve the vulnerability.

(3) **Name**: phpMyAdmin Remote Code Execution, aka CVE-2013-3238
   a. **Description**: a critical vulnerability that allows remote attackers to execute code through the `preg_replace` function call within the “Replace table prefix” feature.
   b. **Impact**: remote attackers could access sensitive information, damaging confidentiality, integrity, and availability of information.
   c. **Actions/Measures**: apply the following patches: drop unsafe usage of pre_replace and prevent null-byte injection in preg_replace.

Stated actions/measures will be taken to address the vulnerabilities in our systems.

Regards,

Team13