# Advisory Alert

**Alert Number:** AAA20210517 **Date:** May 17, 2021

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **WordPress** | **Critical** | **Object Injection vulnerability** |
| IBM QRadar | **Medium** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **WordPress** |
| Severity | **Critical** |
| Affected Vulnerability | Object Injection vulnerability (CVE-2020-36326, CVE-2018-19296) |
| Description | WordPress has released Security Updates addressing object injection vulnerability that exists with PHP mailer.<br><br>CVE-2020-36326 - This vulnerability allows object injection through Phar Deserialization via addAttachment with a UNC pathname. Note: this flaw is similar to CVE-2018-19296, but it came up because 6.1.8 fixed a functionality problem in which UNC pathnames were always considered unreadable by PHPMailer, even in safe contexts. This fix eliminated the code that blocked addAttachment exploitation as an unintended side effect.<br><br>WordPress recommends to apply necessary security fixes at earliest to avoid issues. |
| Affected Products | WordPress versions between 3.7 and 5.7 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/ |

| | |
|---|---|
| Affected Product | IBM QRadar |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2021-20391, CVE-2021-20393) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exists in IBM QRadar.<br><br>CVE-2021-20391: Vulnerability that exists in User Behavior Analytics application leads to cache-able SSL pages that allows web pages to be stored locally which can be read by another user on the system.<br><br>CVE-2021-20393: Successful exploitation of this flaw leads a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser which can be used in further attacks against the particular system. |
| Affected Products | QRadar User Behavior Analytics - 1.0.0-4.1.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/6453103<br>https://www.ibm.com/support/pages/node/6453109 |

## Disclaimer

**The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.**