Advisory Alert

Alert Number : AAA20210412 **Date :** April 12, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Python	**High**	**Denial of Service**
IBM	**High**	**Multiple Vulnerabilities**

Description

Affected Product	**Python**
Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2021-3426)
Description	The ReDoS vulnerable regex has quadratic worst case complexity and it allows cause a denial of service when identifying crafted invalid RFCs. This ReDoS issue is on the client side and needs remote attackers to control the HTTP server. A remote attacker could exploit this vulnerability to trigger spoofing and disclose sensitive information on the targeted system.
Affected Products	Python version prior to 3.9.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.python.org/3/whatsnew/changelog.html

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26296)
Description	Apache MyFaces is vulnerable to cross site request forgery, caused by improper validation of user-supplied input. By persuading an authenticated user to visit a malicious Web site, a remote attacker could send a malformed HTTP request to perform unauthorized actions. An attacker could exploit this vulnerability to perform cross site scripting attacks, Web cache poisoning and other malicious activities.
Affected Products	WebSphere Application Server Liberty 17.0.0.3 – 21.0.0.3 WebSphere Application Server 9.0 WebSphere Application Server 8.5 WebSphere Application Server 8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6441433

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.