Advisory Alert

Alert Number : AAA20210408 **Date :** April 8, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	**Multiple Vulnerabilities**
IBM	**High**	**Server side Request Forgery vulnerability (CVE-2021-20480)**

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Cisco has released security patch updates addressing vulnerabilities that exist in their products such as Cross-Site Scripting, Remote Command Execution, Authorization Bypass, HTML Injection, Command Injection etc. Cisco recommends installing necessary patch updates at earliest to avoid issues.
Affected Products	Multiple Cisco products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&last_published=2021%20Apr&sort=-last_published#~Vulnerabilities

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Server side Request Forgery vulnerability (CVE-2021-20480)
Description	IBM Web Sphere Application Server is vulnerable to SSRF. By sending specific crafted requests, A remote attacker could exploit this issue which provide access to sensitive data. However in order to fix this issue, addressed packages have to be upgraded.
Affected Products	WebSphere Application Server 7.0 WebSphere Application Server 8.0 WebSphere Application Server 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6441063

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.