Advisory Alert

Alert Number: AAA20220517 **Date:** May 18, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Medium**	Policy Bypass Vulnerability
IBM	**Medium**	Spoofing vulnerability

Description

Affected Product	Cisco
Severity	**Medium**
Affected Vulnerability	Policy Bypass Vulnerability (CVE-2021-1236)
Description	Cisco has released security updates addressing a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on multiple affected cisco products. Due to a flaw in the detection algorithm, an attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. Successful exploitation could lead the attacker to bypass the configured policies and deliver a malicious payload to the protected network.
Affected Products	3000 Series Industrial Security Appliances (ISAs) Firepower Threat Defe 1000 Series Integrated Services Routers (ISRs) 4000 Series Integrated Services Routers (ISRs) Cloud Services Router 1000V Integrated Services Virtual Router (ISRv)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq

Affected Product	IBM
Severity	**Medium**
Affected Vulnerability	Spoofing vulnerability (CVE-2022-22475)
Description	IBM has released security updates addressing vulnerability which exists in IBM WebSphere Application Server Liberty with identity spoofing with the appSecurity-1.0, appSecurity-2.0, appSecurity-3.0 or appSecurity-4.0 feature enabled. IBM strongly recommends to apply necessary fixes at earliest to avoid issues.
Affected Products	IBM WebSphere Application Server Liberty 17.0.0.3 – 22.0.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6586734

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.