Advisory Alert

Alert Number: **AAA20240722** **Date:** **July 22, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Cisco	**High**	Protocol Spoofing Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-32760, CVE-2020-15257)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2021-32760 -** Containerd could allow a remote attacker to gain elevated privileges on the system, caused by improper file permissions. By pulling and extracting a specially-crafted container image, an attacker could exploit this vulnerability to perform Unix file permission changes for existing files in the host's filesystem. **CVE-2020-15257 -** Containerd could allow a remote authenticated attacker to gain elevated privileges on the system, caused by improper access control in containerd-shim API. By sending a specially-crafted request, an attacker could exploit this vulnerability to cause new processes to be run with elevated privileges. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Ceph - Versions 7.0z1 - z2, 6.1z1 - z6, 6.0, 5.3z1 - z6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7160780

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Protocol Spoofing Vulnerability (CVE-2024-3596)
Description	Cisco has release security update addressing a RADIUS Protocol Spoofing Vulnerability that exists in their products. These vulnerabilities could allow malicious users to forgery attacks by an on-path attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Network and Content Security Devices • Adaptive Security Appliance (ASA) • Firepower Device Manager (FDM) • Firepower Management Center (FMC) Software • Identity Services Engine (ISE) • Secure Email Gateway • Secure Email and Web Manager • Secure Firewall • Secure Network Analytics • Secure Web Appliance Network Management and Provisioning • Nexus Dashboard, formerly Application Services Engine Routing and Switching - Enterprise and Service Provider • IOS XE Software • IOx Fog Director • MDS 9000 Series Multilayer Switches • Nexus 3000 Series Switches • Nexus 7000 Series Switches • Nexus 9000 Series Switches in standalone NX-OS mode Unified Computing • UCS Central Software • UCS Manager ***To determine the exposure and affected versions, use the Cisco Bug Search Tool.**
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-21285, CVE-2021-31525, CVE-2021-3121, CVE-2022-34038, CVE-2021-41103, CVE-2021-41089, CVE-2020-29652, CVE-2022-27536, CVE-2021-44716, CVE-2023-28842, CVE-2021-21284, CVE-2021-30465, CVE-2018-16875, CVE-2022-24769, CVE-2022-21698, CVE-2021-41091, CVE-2022-36109, CVE-2022-27191, CVE-2021-43565, CVE-2023-5363, CVE-2024-25062, CVE-2023-39615, CVE-2023-45322, CVE-2023-45803, CVE-2023-43804, CVE-2024-21319, CVE-2023-51043, CVE-2021-23566)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may compromise the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Ceph – Versions • 6.0 • 7.0 • 7.1 • 5.3z1 - z6 • 6.1z1 - z6 • 7.0z1 - z2 IBM Storage Protect Plus Server - Versions 10.1.0 - 10.1.16.1 on Linux
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7160780 • https://www.ibm.com/support/pages/node/7160796 • https://www.ibm.com/support/pages/node/7160793 • https://www.ibm.com/support/pages/node/7160790 • https://www.ibm.com/support/pages/node/7160782 • https://www.ibm.com/support/pages/node/7160721 • https://www.ibm.com/support/pages/node/7160784

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Arbitrary code Execution, Denial of Service, NULL Pointer Dereference, Integer Overflow. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 20.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6895-3 • https://ubuntu.com/security/notices/USN-6898-3

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.