Advisory Alert

Alert Number: AAA20240619 **Date:** June 19, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware Broadcom	**Critical**	Multiple Vulnerabilities
IBM	**Low**	Multiple Vulnerabilities

Description

Affected Product	**VMware Broadcom**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-37079, CVE-2024-37080, CVE-2024-37081)
Description	Broadcom has issued security updates addressing multiple vulnerabilities that exist in VMware vCenter Server and VMware Cloud Foundation. These vulnerabilities could be exploited by malicious users to cause heap-overflow and privilege escalation. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware vCenter Server 8.0 VMware vCenter Server 7.0 Cloud Foundation (vCenter Server) 5.x Cloud Foundation (vCenter Server) 4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453

Affected Product	**IBM**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45853, CVE-2023-29267, CVE-2024-25710, CVE-2024-26308, CVE-2023-45178, CVE-2024-28762, CVE-2024-28757, CVE-2024-29025, CVE-2024-29131, CVE-2024-29133, CVE-2024-31880, CVE-2024-31881)
Description	IBM has issued security updates addressing multiple vulnerabilities that exist in IBM WebSphere Remote Server. If exploited, these vulnerabilities could lead to Denial Of Service, Execute Arbitrary Code and Sensitive Information Disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Remote Server 9.1, 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7157880

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.