Advisory Alert

Alert Number: **AAA20241212** **Date:** **December 12, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Authentication Bypass Vulnerability
Synology	**High**	Security Update
Ivanti	**High**	Multiple Privilege Escalation Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Dell	**High**	Plain-text Password Storage Vulnerability
Drupal	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2024-51504)
Description	IBM has released security updates addressing an Authentication Bypass Vulnerability that exists in their products. **CVE-2024-51504** - Apache ZooKeeper could allow a remote attacker to bypass security restrictions, caused by a flaw when using IPAuthenticationProvider. By spoofing client's IP address in request headers, an attacker could exploit this vulnerability to bypass authentication. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM Versions - 7.5 - 7.5.0 UP10 IF01 QRadar Incident Forensics Versions - 7.5 - 7.5.0 UP10 IF01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7178556

Affected Product	**Synology**
Severity	**High**
Affected Vulnerability	Security Update
Description	Synology has released security updates addressing a vulnerability that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Synology Media Server for DSM 7.2 Versions Prior to 2.2.0-3325 Synology Media Server for DSM 7.1 Versions Prior to 2.0.5-3152 Synology Media Server for SRM 1.3 Versions Prior to 1.4-2680
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_24_28

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Privilege Escalation Vulnerabilities (CVE-2024-8496, CVE-2024-10251, CVE-2024-9845, CVE-2024-11597)
Description	Ivanti has released security updates addressing Multiple Privilege Escalation Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Workspace Control Version 10.18.30.0 and prior Ivanti Security Controls Version 2024 and prior Ivanti Automation Version 2024.4 and prior Ivanti Performance Manager Version 2024.3 Ivanti Performance Manager Version 2024.1 Ivanti Performance Manager Version 2023.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/December-2024-Security-Advisory-Ivanti-Workspace-Control-IWC-CVE-2024-8496?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Security-Controls-iSec-CVE-2024-10251?language=en_US • https://forums.ivanti.com/s/article/December-2024-Security-Advisory-Ivanti-Automation-CVE-2024-9845?language=en_US • https://forums.ivanti.com/s/article/December-2024-Security-Advisory-Ivanti-Performance-Manager-CVE-2024-11597?language=en_US

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24968, CVE-2024-24853, CVE-2023-43753, CVE-2024-21781, CVE-2024-21829, CVE-2024-23599, CVE-2024-21853, CVE-2024-22185, CVE-2024-24985, CVE-2024-25565, CVE-2024-21820, CVE-2024-23918, CVE-2023-31315, CVE-2024-21850, CVE-2024-23984)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, Privilege Escalation, Denial of Service, Escalation of Privilege. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE SimpliVity 380 Gen10 Plus - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_1129 HPE SimpliVity 380 Gen11 - Prior to HPE SimpliVity Gen11 Support Pack (SVTSP) v2024_1129 HPE SimpliVity 170r Gen10 Server - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_1129 HPE SimpliVity 190r Gen10 Server - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_1129 HPE SimpliVity 380 Gen10 - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_1129 HPE SimpliVity 380 Gen10 G - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_1129 HPE SimpliVity 380 Gen10 H - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_1129 HPE SimpliVity 325 Gen10 - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_1129 HPE SimpliVity 325 Gen10 Plus - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_1129 HPE SimpliVity 325 Gen11 - Prior to HPE SimpliVity Gen11 Support Pack (SVTSP) v2024_1129
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04752en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04690en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04753en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04751en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04754en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04755en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04756en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04686en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04757en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04743en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Plain-text Password Storage Vulnerability (CVE-2024-53292)
Description	Dell has released security updates addressing a Plain-text Password Storage Vulnerability that exists in their products. **CVE-2024-53292 -** Dell VxVerify, versions prior to x.40.405, contain a Plain-text Password Storage Vulnerability in the shell wrapper. A local high privileged attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable component with privileges of the compromised account. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VxRail VxVerify Versions prior to x.40.405
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000258964/dsa-2024-492-security-update-dell-vxverify-on-vxrail-plaintext-password-storage-vulnerabilities

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to cause Access Bypass and Cross-site Scripting Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Login Disable module Versions prior to 2.1.1 for Drupal 9.x / 10.x Browser Back Button module Versions prior to 2.0.2 for Drupal 9.x / 10.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-073 • https://www.drupal.org/sa-contrib-2024-072

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-23454, CVE-2022-40152, CVE-2023-35116, CVE-2024-45491, CVE-2024-52318, CVE-2023-36478, CVE-2023-44487, CVE-2024-52317, CVE-2024-52316, CVE-2023-31582, CVE-2019-12900, CVE-2024-3596, CVE-2023-34453, CVE-2023-34454, CVE-2023-34455, CVE-2023-43642, CVE-2023-2976, CVE-2020-8908, CVE-2023-33546, CVE-2022-41881, CVE-2022-41915, CVE-2023-34462, CVE-2022-3171, CVE-2021-22569, CVE-2024-10041, CVE-2024-10963)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Denial of Service, Authentication Bypass, Arbitrary Code Execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM Versions - 7.5 - 7.5.0 UP10 IF01 QRadar Incident Forensics Versions - 7.5 - 7.5.0 UP10 IF01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7178556

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.