Advisory Alert

Alert Number: AAA20260630 **Date:** June 30, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
HPE	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-1525, CVE-2025-62718, CVE-2026-4800, CVE-2026-22732, CVE-2026-29063, CVE-2026-33186, CVE-2026-41691, CVE-2026-2332, CVE-2026-40976, CVE-2025-68121, CVE-2026-33896, CVE-2026-27148, CVE-2026-33937, CVE-2026-42043, CVE-2026-42044, CVE-2025-61140, CVE-2026-1615, CVE-2026-27837, CVE-2026-33228)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Business Automation: • V25.0.1 - V25.0.1-IF001 • V25.0.0 - V25.0.0-IF004 • V24.0.1 - V24.0.1-IF007 • V24.0.0 - V24.0.0-IF008 IBM Business Automation Workflow containers: • V25.0.1 - V25.0.1-IF001 • V25.0.0 - V25.0.0-IF004 • V24.0.1 - V24.0.1-IF007
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7278246 https://www.ibm.com/support/pages/node/7278337

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-12543, CVE-2025-23184, CVE-2025-9784, CVE-2024-29371, CVE-2026-31411, CVE-2026-43198, CVE-2026-46331, CVE-2026-46243)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:33372 https://access.redhat.com/errata/RHSA-2026:33371 https://access.redhat.com/errata/RHSA-2026:33285 https://access.redhat.com/errata/RHSA-2026:33224 https://access.redhat.com/errata/RHSA-2026:33222 https://access.redhat.com/errata/RHSA-2026:33221 https://access.redhat.com/errata/RHSA-2026:33220 https://access.redhat.com/errata/RHSA-2026:33219

Vendor	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-30513, CVE-2025-31944, CVE-2025-32007, CVE-2025-32467, CVE-2025-27572, CVE-2025-27940, CVE-2025-29950, CVE-2024-21961, CVE-2025-48514, CVE-2025-29939, CVE-2025-0031, CVE-2025-52536, CVE-2025-48509, CVE-2025-21953, CVE-2025-52533, CVE-2024-36310, CVE-2024-36355, CVE-2025-31648)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• HPE SimpliVity 380 Gen11 - Prior to SimpliVity Gen11 Support Pack (SVTSP) 2026-0605 • HPE SimpliVity 325 Gen10 - Prior to SimpliVity Gen10 Support Pack (SVTSP) 2026-0605 • HPE SimpliVity 325 Gen10 Plus - Prior to SimpliVity Gen10 Support Pack (SVTSP) 2026-0605 • HPE SimpliVity 325 Gen11 - Prior to SimpliVity Gen11 Support Pack (SVTSP) 2026-0605 • HPE SimpliVity 380 Gen11 - Prior to SimpliVity Gen11 Support Pack 2026_0605 • HPE SimpliVity 380 Gen10 Plus - Prior to SimpliVity Gen10 Support Pack 2026_0605
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05019en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05020en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05017en_us&docLocale=en_US

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Business Automation: • V25.0.1 - V25.0.1-IF001 • V25.0.0 - V25.0.0-IF004 • V24.0.1 - V24.0.1-IF007 • V24.0.0 - V24.0.0-IF008 IBM Business Automation Workflow containers: • V25.0.1 - V25.0.1-IF001 • V25.0.0 - V25.0.0-IF004 • V24.0.1 - V24.0.1-IF007
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7278246 https://www.ibm.com/support/pages/node/7278337 https://www.ibm.com/support/pages/node/7278340

Vendor	**F5**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22869, CVE-2025-4673)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-22869**: SSH servers which implement file transfer protocols are vulnerable to a denial of service attack from clients which complete the key exchange slowly, or not at all, causing pending content to be read into memory, but never transmitted **CVE-2025-4673**: Proxy-Authorization and Proxy-Authenticate headers persisted on cross-origin redirects potentially leaking sensitive information. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	F5OS-A: 1.8.0 - 1.8.3 1.5.1 - 1.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000161970 https://my.f5.com/manage/s/article/K000161965

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.