Advisory Alert

Alert Number: **AAA20231027** **Date:** **October 27, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**Critical**	Remote code execution vulnerability
Red Hat	**High**	Denial of service vulnerability
IBM	**High**	Arbitrary code execution vulnerability
F5	**High**	SQL injection vulnerability
VMware	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
Synology	**Low**	Buffer Overflow vulnerability

Description

Affected Product	**F5**
Severity	**Critical**
Affected Vulnerability	Remote code execution vulnerability (CVE-2023-46747)
Description	F5 has released a critical security update addressing Remote code execution vulnerability. By exploiting this vulnerability, an unauthenticated attacker with network access to the BIG-IP system through the management port and/or self-IP addresses can execute arbitrary system commands. F5 highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	BIG-IP 17.1.0 BIG-IP 16.1.0 - 16.1.4 BIG-IP 15.1.0 - 15.1.10 BIG-IP 14.1.0 - 14.1.5 BIG-IP 13.1.0 - 13.1.5 BIG-IP Configuration utility
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000137368 https://my.f5.com/manage/s/article/K000137353

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Denial of service vulnerability (CVE-2023-44487)
Description	Red Hat has released security updates addressing Denial of service vulnerability in their products. **CVE-2023-44487** -A flaw was found in handling multiplexed streams in the HTTP/2 protocol. A client can repeatedly make a request for a new multiplex stream and immediately send an RST_STREAM frame to cancel it. This flow can lead to denial of service due to server resource consumption Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat JBoss Core Services Text-Only Advisories x86_64 Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services 1 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:6106 https://access.redhat.com/errata/RHSA-2023:6105

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Arbitrary code execution vulnerability (CVE-2023-30431)
Description	IBM has released security updates addressing Arbitrary code execution vulnerability due to buffer overflow, caused by improper bounds checking in IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) db2set. A local attacker can create a specially crafted file, trigger memory corruption and execute arbitrary code on the target system. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Db2 10.5.0.11 Server IBM Db2 11.1.4.7 Server IBM Db2 11.5.x Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7010565

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	SQL injection vulnerability (CVE-2023-46748)
Description	F5 has released security updates addressing SQL injection vulnerability in their products which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. F5 recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	BIG-IP 17.1.0 BIG-IP 16.1.0 - 16.1.4 BIG-IP 15.1.0 - 15.1.10 BIG-IP 14.1.0 - 14.1.5 BIG-IP 13.1.0 - 13.1.5 BIG-IP Configuration utility
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000137365 https://my.f5.com/manage/s/article/K000137368

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34057, CVE-2023-34058)
Description	VMware has released a security update addressing Local Privilege Escalation and SAML Token Signature Bypass vulnerabilities in VMware Tools . **CVE-2023-34057-** A local privilege escalation vulnerability in VMware Tools for macOS .By exploiting this vulnerability, a local user who has access to a guest virtual machine may elevate privileges within the virtual machine. **CVE-2023-34058-** A SAML Token Signature Bypass vulnerability in VMware Tools. A remote attacker with guest operation privileges on a virtual machine may be able to elevate their privileges if the virtual machine has been assigned to more privileged Guest Alias. VMware recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	VMware Tools 12.x.x, 11.x.x, 10.3.x running on macOS VMware Tools 12.x.x, 11.x.x, 10.3.x running on Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0024.html

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4244, CVE-2023-42752, CVE-2023-42753, CVE-2023-42755, CVE-2023-42756, CVE-2023-4622, CVE-2023-4623, CVE-2023-4881, CVE-2023-4921, CVE-2023-5197, CVE-2023-34319)
Description	Ubuntu has released security update addressing Multiple Vulnerabilities in their products. Successful exploitation of these vulnerabilities could lead to Denial of Service and Arbitrary code Execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 20.04 LTS Ubuntu 23.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6446-3 https://ubuntu.com/security/notices/USN-6454-1

Affected Product	**Synology**
Severity	**Low**
Affected Vulnerability	Buffer Overflow vulnerability (CVE-2023-5748)
Description	Synology has released a security update addressing Buffer Overflow vulnerability in the Synology SSL VPN Client. Buffer copy without checking the size of the input in cgi component allows local users to conduct denial-of-service attacks via unspecified vectors. Synology recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Synology SSL VPN Client versions before 1.4.7-0687
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_23_12

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.