Advisory Alert

Alert Number: AAA20231108 **Date:** November 8, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Multiple Vulnerabilities
Commvault	**Critical**	Remote Code Execution Vulnerability
Ivanti	**High**	Privilege escalation vulnerability
OpenSSL	**Low**	Denial of Service Vulnerability

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22893, CVE-2021-22894, CVE-2021-22899, CVE-2021-22900)
Description	Ivanti has released security updates addressing the Multiple critical vulnerabilities in Pulse Connect Secure. **CVE-2021-22893** - Multiple use after free in PCS before 9.1R11.4 allows a remote unauthenticated attacker to execute arbitrary code via license server web services. **CVE-2021-22894** - Buffer overflow in PCS Collaboration Suite before 9.1R11.4 allows a remote authenticated user to execute arbitrary code as the root user via maliciously crafted meeting room. **CVE-2021-22899** - Command Injection in PCS before 9.1R11.4 allows a remote authenticated user to perform remote code execution via Windows File Resource Profiles. **CVE-2021-22900** - Multiple unrestricted uploads in PCS before 9.1R11.4 allow an authenticated administrator to perform a file write via a maliciously crafted archive upload in the administrator web interface Ivanti recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Pulse Connect Secure versions prior to 9.1R11.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/SA44784?language=en_US

Affected Product	**Commvault**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2023-46604)
Description	Commvault has released a security update addressing a Remote Code Execution Vulnerability in third party component Apache ActiveMQ used in Commvault Web Server. The vulnerability exists due to insecure input validation when processing serialized data in the OpenWire protocol. A remote attacker can pass specially crafted data to the application and execute arbitrary code on the target system. Commvault recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Commvault Web Server Platform Release 2023E, 2023, 2022E
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/v11/essential/146231_security_vulnerability_and_reporting.html

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Privilege escalation vulnerability (CVE-2023-38041)
Description	Ivanti has released a security update addressing privilege escalation vulnerability that exist in Ivanti Secure Access Client Below 22.6R1 on Windows user machines. Ivanti recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Ivanti Secure Access Client Below 22.6R1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/CVE-2023-38041-New-client-side-release-to-address-a-privilege-escalation-on-Windows-user-machines?language=en_US

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-5678)
Description	OpenSSL released a security update addressing Denial of Service Vulnerability exists in their products. Due to improper management of internal resources within the DH_generate_key() and DH_check_pub_key() functions, a remote attacker can pass specially crafted data to the application and perform a denial-of-service attack. OpenSSL recommends to apply the necessary fixes at your earliest to avoid issues.
Affected Products	OpenSSL 3.1, 3.0, 1.1.1 and 1.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20231106.txt

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.