# Alert Bulletin

**Bulletin N.:** 2024-37
**Publication Date:** 20/09/2024
**Subject:** Alert 2024-37 Critical Vulnerabilities in Ivanti CSA CVE-2024-8963 and CVE-2024-8190
**Traffic Light Protocol (TLP):** White

## Affected Product(s):

- CSA 4.6 (all versions prior to patch 519)

## Description:

Ivanti has disclosed a new critical vulnerability in its Cloud Services Appliance (CSA) version 4.6, which was resolved in CSA 4.6 Patch 519, released on September 10. The vulnerability, identified as CVE-2024-8963, allows an unauthenticated remote attacker to access restricted functionalities through successful exploitation.

This risk is elevated when combined with CVE-2024-8190, as the attacker could bypass admin authentication and execute arbitrary commands on affected devices. CVE-2024-8190, a previously disclosed OS command injection vulnerability with a CVSS score of 7.2, required admin-level authentication. However, with CVE-2024-8963, the attacker can bypass this condition by exploiting both vulnerabilities together.

Ivanti has confirmed limited exploitation of these vulnerabilities and strongly recommends all users update to CSA version 5.0. It's important to note that version 4.6 has reached end-of-life and no longer receives support, meaning any system still operating on this version is at risk of exploitation.

Additionally, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) urges administrators to review Ivanti's security advisory and apply the necessary updates to mitigate the risks posed by these vulnerabilities. Exploitation of these flaws could lead to remote code execution on affected devices, posing a serious threat to enterprise security.