

CISA Adds Two New Vulnerabilities to KEV Catalog



CISA has added two vulnerabilities to its Known Exploited Vulnerabilities Catalog, highlighting the need for organizations to prioritize remediation efforts for these risks.

- CISA has identified two new vulnerabilities: a Microsoft Windows Command Injection and an Ivanti Connect Secure Authentication Bypass.
- These vulnerabilities are actively exploited and pose significant risks.
- Organizations are encouraged to adopt risk-based vulnerability management.
- Rapid remediation of high-risk vulnerabilities is essential.
- CISA will continue to update the KEV Catalog with new vulnerabilities.

Overview

CISA has added two vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, which indicates active exploitation. The vulnerabilities include a **Command Injection** vulnerability in Microsoft Windows and an **Authentication Bypass** vulnerability in Ivanti Connect Secure. These vulnerabilities are common attack vectors for cybercriminals and present significant risks to organizations.

Recommendations

While the Binding Operational Directive (BOD) 26-04 applies to federal agencies, it underscores the importance of prioritizing remediation for high-risk vulnerabilities. Organizations are encouraged to adopt similar practices in their own vulnerability management processes. This includes assessing the risk associated with each vulnerability and prioritizing remediation efforts accordingly.

Next Steps

Organizations should ensure they are aware of these vulnerabilities and take appropriate actions to mitigate risks. Regularly reviewing the KEV Catalog for updates is essential to maintain a robust security posture.

What to do now

1. Review the CISA KEV Catalog for the latest vulnerabilities.
2. Assess the impact of the newly identified vulnerabilities on your systems.
3. Prioritize remediation efforts for these vulnerabilities based on risk.
4. Implement security patches as soon as they are available.
5. Conduct regular vulnerability assessments to identify potential risks.