

Advisory on Citrix NetScaler Vulnerabilities



The NCSC has identified vulnerabilities in Citrix NetScaler ADC and Gateway, with two actively exploited. Organizations should take immediate action to mitigate risks.

- Eight vulnerabilities have been identified in Citrix NetScaler ADC and Gateway.
- Two vulnerabilities are actively being exploited.
- Affected organizations should review the Citrix security bulletin.
- Immediate isolation and updating of affected systems is recommended.
- Continuous monitoring and threat hunting should be implemented.

Overview

The National Cyber Security Centre (NCSC) has issued a warning regarding vulnerabilities in Citrix NetScaler

ADC and Citrix NetScaler Gateway. These vulnerabilities pose significant risks, particularly as two of them are confirmed to be actively exploited by attackers.

Affected Systems

Organizations utilizing Citrix NetScaler ADC or Gateway should be aware that specific versions are vulnerable. It is crucial to assess whether your systems fall under the affected categories and take appropriate actions to mitigate potential risks.

Recommended Actions

To safeguard your organization, consider the following actions:

- Review the Citrix security bulletin for detailed information on the vulnerabilities.
- Isolate any affected systems and replace them with updated versions if possible.
- Investigate for signs of compromise using the indicators of compromise (IoCs) provided by Citrix.
- Install the latest updates as recommended by Citrix to patch vulnerabilities.
- Continuously monitor for threats and utilize tools like NetScaler Console File Integrity Monitoring to detect unauthorized changes.

What to do now

1. Review the Citrix security bulletin.
2. Isolate affected systems and consider replacing them.
3. Investigate for signs of compromise using IoCs.
4. Install the latest updates from Citrix.
5. Monitor for threats continuously.