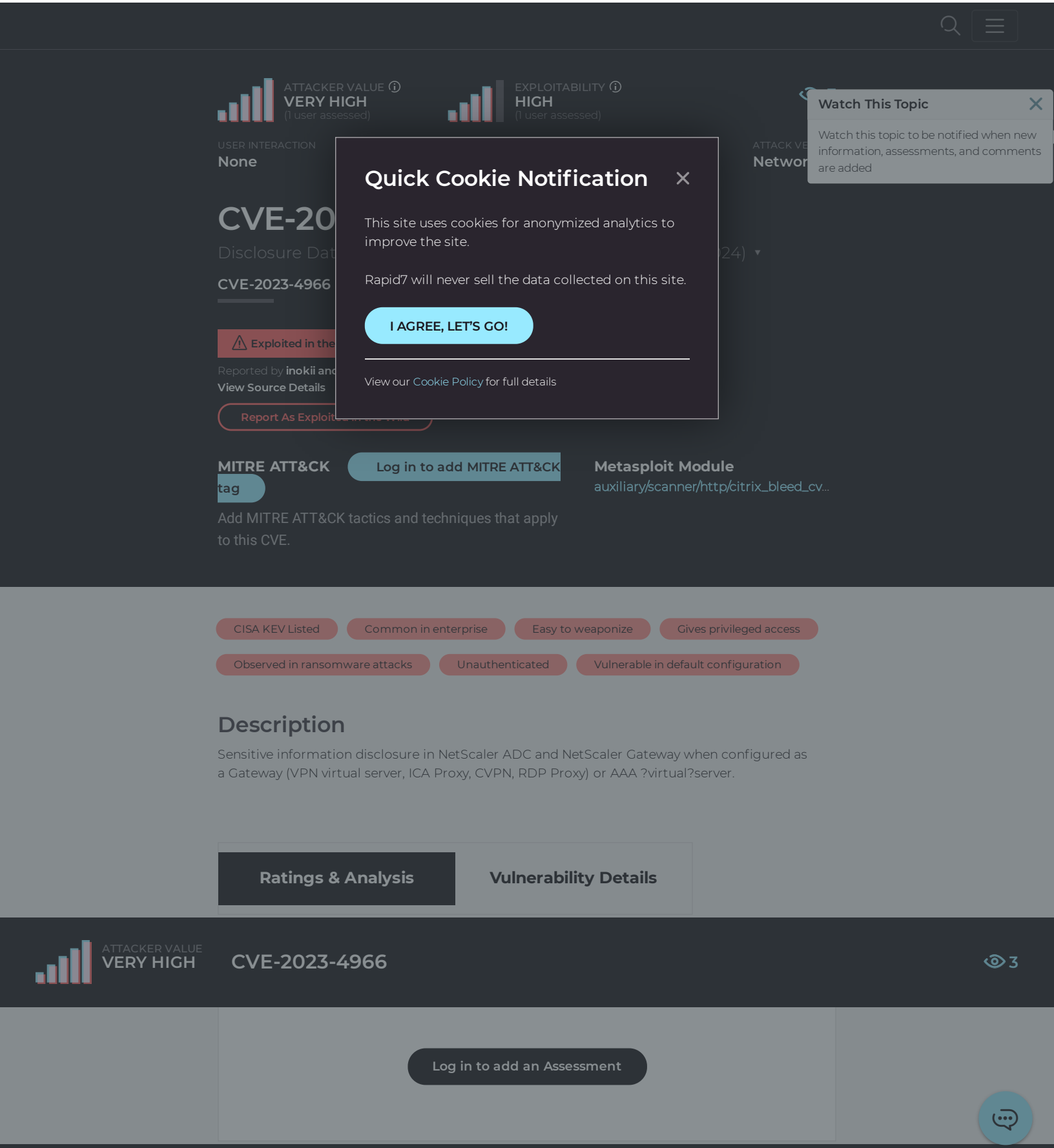
ATTACKER VALUE
VERY HIGH
(1 user assessed)
EXPLOITABILITY
HIGH
(1 user assessed)
Watch This Topic
Watch this topic to be notified when new information, assessments, and comments are added
USER INTERACTION
None
Quick Cookie Notification
This site uses cookies for anonymized analytics to improve the site.
Rapid7 will never sell the data collected on this site.
I AGREE, LET'S GO!
View our Cookie Policy for full details
CVE-2023-4966
Exploited in the
View Source Details
MITRE ATT&CK tag
Log in to add MITRE ATT&CK
Add MITRE ATT&CK tactics and techniques that apply to this CVE.
Metasploit Module
auxiliary/scanner/http/citrix_bleed_cv...
CISA KEV Listed
Common in enterprise
Easy to weaponize
Gives privileged access
Observed in ransomware attacks
Unauthenticated
Vulnerable in default configuration
Description
Sensitive information disclosure in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA ?virtual?server.
Ratings & Analysis
Vulnerability Details
ATTACKER VALUE
VERY HIGH
CVE-2023-4966
3
Log in to add an Assessment
This site uses cookies for anonymized analytics. For more information or to change your cookie settings, view our Cookie Policy.

6

rbowes-r7 (95) 20

October 24, 2023 6:01pm UTC (1 year ago) • Edited 8 months ago

Ratings

ATTAC

EXPLO

ion

Techn

On Oc erability in Citrix ADC, which affects the following versions:

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.15
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.19
- NetScaler ADC 13.1-FIPS before 13.1-37.164
- NetScaler ADC 12.1-FIPS before 12.1-55.300

See More

Log in to Add Reply

Quick Cookie Notification

This site uses cookies for anonymized analytics to improve the site.

Rapid7 will never sell the data collected on this site.

View our Cookie Policy for full details