Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 241 **07-03-2024**

Name: Critical Vulnerability in Cisco Duo for Windows Logon and RDP

Threat Classification: Authentication Bypass / Security Vulnerability

Affected Software / Services:

- Cisco Duo Authentication for Windows Logon and RDP versions 4.2.0 through 4.2.2

Summary:

A critical security vulnerability, identified as CVE-2024-20301, has been uncovered in Cisco Duo Authentication for Windows Logon and Remote Desktop Protocol (RDP). This vulnerability allows an authenticated, local attacker to bypass secondary authentication mechanisms, gaining unauthorized access to Windows devices. The flaw arises due to a failure to invalidate locally created trusted sessions after a device reboot, providing an avenue for attackers with primary user credentials to exploit this weakness. Systems running versions earlier than 4.2.0 or the latest patched version, 4.3.0, are not vulnerable to this exploit. Cisco has responded with software updates, and customers are urged to promptly update affected systems.

Severity	Critical
Attack Vector	Local Authentication Bypass

© Copyright 2023, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.

Recommendations:

- Update affected systems to the latest software release promptly.
- Reset the registry key on affected devices by following Cisco's recommended process.
- Refer to Cisco's provided resources for detailed instructions on resetting the secret key for a Duo-Protected Application or Directory Sync.
- For more information and recommendation pls visit Cisco for Windows and RDP Let Attacker Bypass Authentication (cybersecuritynews.com)
- In case of any incident, please report to this office, through PTA CERT Portal and email.

© Copyright 2023, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.