مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Google Quick Share utility

Tracking #:432316141

Date:13-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Google's Quick Share data transfer utility that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Multiple vulnerabilities have been identified in Google's Quick Share data transfer utility for Android and Windows. These vulnerabilities, collectively known as "QuickShell," can be exploited to achieve remote code execution (RCE) on affected systems.

Vulnerabilities Details:

- **CVE-2024-38271**
  - Vulnerability exists in Quick Share/Nearby that Forces a victim to stay connected to a temporary Wi-Fi connection created for sharing.
  - CVSS Score 5.9 Medium
- **CVE-2024-38272**
  - Vulnerability exists in Quick Share/Nearby that allows an attacker to bypass the accept file dialog on Windows.
  - CVSS Score 7.1 High

Impact:

Successful exploitation of these vulnerabilities could lead to:

- Remote code execution on the victim's device
- Unauthorized file writes
- Denial of service (DoS) conditions
- Man-in-the-middle (MitM) attacks
- Forced Wi-Fi connections

Affected Systems

- Google Quick Share for Android
- Google Quick Share for Windows

Fixed Versions:

Quick Share (1.0.1724.0 or later)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the Google Quick Share to the latest version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-38271
- https://www.cve.org/cverecord?id=CVE-2024-38272