EINPRESSWIRE

Silent Sector Advises IETF of Major Vulnerability Related to QR Codes Used to Enroll Two-Factor Authentication Processes

Millions – Perhaps Tens of Millions – of 2FA Credentials at Risk of Exposure. Global Remediation Likely to Cost Billions of Dollars

SCOTTSDALE, AZ, UNITED STATES, October 2, 2024 /EINPresswire.com/ -- A significant exposure related to the use of QR codes in two-factor authentication (2FA) processes has been identified and reported to the Internet Engineering Task Force (IETF) by researchers and analysts at Silent Sector (https://silentsector.com), a cybersecurity services company that specializes in providing tailored risk management solutions to mid-market and emerging companies across various industries, including healthcare, financial services, technology, manufacturing, and defense.

> “
> Many IT shops, managed service providers (MSPs), as well as other business and technology professionals often store or email these QR codes, leaving them open to discovery. ”
>
> *Brian Contario, Silent Sector*

The exploit, discovered by Brian Contario, Principal Cybersecurity Architect at Silent Sector, lies in the fact that the QR codes used for 2FA enrollment contain sensitive information, including a secret key and user identifiers, which can be captured and misused if not properly secured.

“These codes have been present for over a decade, potentially affecting millions of users worldwide. While this vulnerability is not widely recognized, once it becomes more widely known, it will likely emerge as an area of focus for malicious actors,” says Contario.

There are a number of ways that bad actors could gain access to the secret key information in the QR codes. Potential caches of the data include email, messaging, or cloud storage repositories where the QR codes or enrollment information have been transmitted or stored.

“Many IT shops, managed service providers (MSPs), as well as other business and technology professionals often store or email these QR codes, leaving them open to discovery. In public places, including airports, cafes and co-working spaces, images of the QR code can be captured simply by using cameras with zoom lenses when QR codes are displayed on screens for enrollment," he says.

Brian Contario, Silent Sector

Scope of the Damage

The potential scale of impact is estimated anywhere from tens to hundreds of millions of affected enrollments. Google Authenticator added support for QR codes approximately 12 years ago.

Millions upon millions of QR code enrollments enabled over the past decade have created a large pool of "data residue" where the digital fingerprints of particular 2FA interactions have been saved and archived.

The enrollment processes were originally designed for hardware security tokens that could securely embed the secret key that were transmitted to physical tokens or other devices.

"However, when this process was adapted for software-based 2FA apps, the secure exchange of the secret key was not properly maintained. As a result, transmitting the QR code can lead to the key being compromised. If attackers gain access to this information, they can potentially use it to bypass the 2FA protection," says Contario. "While the level of awareness of this exploit currently seems to be low – even among IT professionals – the potential for abuse exists," he adds.

Remediation Solution

To address the threat, Silent Sector has developed a fix which involves changing the enrollment process to use a QR code that is paired with a dynamic, one-time URL that directs the authenticator app to retrieve the secret key from a secure server.

"This ensures that the secret key is only sent to the authenticator app, making it more secure. To execute the fix, technology vendors and enterprises that use QR enrollment for multi-factor authentication will need to re-enroll in their 2FA processes using new, secure QR codes," explains Contario.

This way, the secret key is no longer statically embedded in the QR code, but dynamically provided to the authenticator app in a secure manner, preventing the compromise of secure data through the QR code alone.

For the rest of the industry briefing report, please visit: https://bit.ly/3BCCjcq

Lane Cooper
BizTechReports
email us here