The Verify Ontario app is designed to be used by businesses and organizations to scan enhanced vaccine certification QR codes. It provides a quick and easy way to determine if a person meets Ontario's requirements for premises entry, and by extension, determines if the person has received their COVID-19 vaccines.

Each QR code conforms to the Smart Health Cards format, and contains among other things, a person's name, date of birth, and vaccination dates. In order to prevent a person from creating a fake QR code, each QR code is signed with the government's private key. The application uses the Government of Ontario's public key to verify the signature and determine its authenticity. The private key is kept secret, whereas the public key is made available to the app.

Upon scanning a QR code, the application responds with a green "✓" if the signature is valid, and a yellow "!" or red "X" if there was a problem verifying the signature. A green "✓", along with the visitor's ID can permit them entry into the premises.

Verify Ontario versions 1.1 and earlier downloads a list of trusted public keys and rules from <https://files.ontario.ca/apps/verify/verifyRulesetON.json>. These public keys are saved in the app's database. When the app scans a QR code, it uses one of its stored public keys to verify the QR code's signature. If the signature is valid, a green "✓" is displayed.

**Vulnerability Description**

Harold discovered that the Verify Ontario app was vulnerable to a man-in-the-middle attack which could allow an insider threat actor to tamper with the database's public keys, and affect the app's response when scanning a QR code. Utilizing an intercepting proxy, Harold was able to tamper with the list of public keys the app downloaded, and add his own public key to its database. In doing so, any QR code he created and signed with his private key would be verified by the app as valid.

An insider threat scenario could be an employee who adds their public key to the app's database, and distributes QR codes signed with their private key to unvaccinated visitors. Any employee using this tampered device to scan a QR code signed with the threat actor's private key would be reported as valid, and therefore meet Ontario's requirements for premises entry.

**Vulnerable releases**

Android: 1.0.1, 1.1

iOS: 1.0.1, 1.1

**Fixed release**

Android: 1.1.1

iOS: 1.1.1

**Proof of concept**

An insider threat actor would need to follow these steps to tamper with the app's database.

1. Generate their own private and public key pairs for signing their own QR code
2. Create their own QR codes signed with their private key
3. Set up an intercepting proxy. E.g. Burp Suite or mitmproxy
4. Configure the device to be tampered with to use the proxy, and to trust the proxy's SSL certificate
5. Configure the proxy to insert their own public key when the app downloads a list of public keys from <https://files.ontario.ca/apps/verify/verifyRulesetON.json>
6. Update the app's list of public keys by clicking on "Connect for updates". The proxy will intercept the downloaded verifyRulesetON.json, and insert the threat actor's public key into the public key list before it is saved to the app's database
7. Distribute QR codes signed with their public key to anyone who needs access to the premises

**Mitigations**

Verify Ontario version 1.1.1 for Android and iOS now downloads the rules and public keys from <https://files.ontario.ca/apps/verify/verifyRulesetON.jws>. This data is signed with the Government of Ontario's private key, and is checked for authenticity with its matching public key included in the app before it is used. Tampering with the public key list invalidates the signature causing the app to report an error.

**Disclosure timeline**

18 Oct 2021: Discovered vulnerability

19 Oct 2021: Reported vulnerability and proof of concept to appfeedback@ontario.ca

21 Oct 2021: Discussion with Verify Ontario team on vulnerability, remediation, and coordinated disclosure

22 Nov 2021: Version 1.1.1 released which fixes the vulnerability

25 Nov 2021: Public disclosure

**References**

1. Verify Ontario app: <https://covid-19.ontario.ca/verify>
2. Verify Ontario source code on GitHub: <https://github.com/ongov/OpenVerify>
3. Pull request announcing the vulnerability fix: <https://github.com/ongov/OpenVerify/pull/20>
4. Verify Ontario Vulnerability disclosure policy: <https://covid-19.ontario.ca/verify-vulnerability-disclosure>