Talos Vulnerability Report

TALOS-2020-1151

Win-911 mobile server platform privilege escalation vulnerability

JANUARY 4, 2021

CVE NUMBER

CVE-2020-13541

Summary

An exploitable local privilege elevation vulnerability exists in the file system permissions of the Mobile-911 Server V2.5 install directory. Depending on the vector chosen, an attacker can overwrite the service executable and execute arbitrary code with System privileges or replace other files within the installation folder that could lead to local privilege escalation.

Tested Versions

Win-911 Mobile Server V2.5

Product URLs

https://www.win911.com/products/mobile/

CVSSv3 Score

9.3 - CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-276 - Incorrect Default Permissions

Details

WIN-911 Mobile delivers critical SCADA/OT, HMI and control networks alerts to mobile devices in real time. It supports various methods of alert configuration, routing and escalation designed to ensure safety of the environment.

By default, Mobile-911 Server V2.5 is installed in “c:\Program Files (x86)\WIN-911 Software\Mobile-911 Server” directory and it allows “Everyone” group to have “Change” privilege over certain files in the directory which are executed with SYSTEM authority. This allows any user on the system to modify arbitrary files in the install directory resulting in privilege escalation.

```
c:\program files (x86)\win-911 software\mobile-911 server\Mobile911.Server.exe
                                                                                Everyone:C

BUILTIN\Administrators:F

NT AUTHORITY\SYSTEM:(ID)F

BUILTIN\Administrators:(ID)F

BUILTIN\Users:(ID)R

APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(ID)R

APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APP PACKAGES:(ID)R
```

In addition, library files loaded by the service can also be replaced to gain privileged access into the primary Mobile911.Server service executed as Local System:

```
c:\Program Files (x86)\WIN-911 Software\Mobile-911 Server\Mobile911.Common.dll
                                                                                Everyone:C

BUILTIN\Administrators:F

NT AUTHORITY\SYSTEM:(ID)F

BUILTIN\Administrators:(ID)F

BUILTIN\Users:(ID)R

APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(ID)R

APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APP PACKAGES:(ID)R

c:\Program Files (x86)\WIN-911 Software\Mobile-911 Server\System.Data.SQLite.dll
                                                                                Everyone:C

BUILTIN\Administrators:F

NT AUTHORITY\SYSTEM:(ID)F

BUILTIN\Administrators:(ID)F

BUILTIN\Users:(ID)R

APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(ID)R

APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APP PACKAGES:(ID)R

c:\Program Files (x86)\WIN-911 Software\Mobile-911 Server\x64\SQLite.Interop.dll
                                                                                Everyone:C

BUILTIN\Administrators:F

Everyone:(ID)C

BUILTIN\Administrators:(ID)F

NT AUTHORITY\SYSTEM:(ID)F

BUILTIN\Users:(ID)R

APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(ID)R

APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APP PACKAGES:(ID)R

c:\Program Files (x86)\WIN-911 Software\Mobile-911 Server\x86\SQLite.Interop.dll
                                                                                Everyone:(ID)C

BUILTIN\Administrators:(ID)F

NT AUTHORITY\SYSTEM:(ID)F

BUILTIN\Users:(ID)R

APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(ID)R
```

Credit

Discovered by Yuri Kramarz of Cisco Talos.

https://talosintelligence.com/vulnerability_reports/

Timeline

2020-09-01 - Vendor Disclosure
2020-09-02 - Vendor confirmed support ticket issued
2020-11-04 - 60 day follow up
2020-12-09 - 90 day follow up
2021-01-04 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.
