Talos Vulnerability Report

TALOS-2020-1150

Win-911 Enterprise Platform privilege escalation vulnerability

JANUARY 4, 2021

CVE NUMBER

CVE-2020-13539, CVE-2020-13540

Summary

Multiple exploitable local privilege elevation vulnerability exists in the file system permissions of the Win-911 Enterprise V4.20.13 install directory. Depending on the vector chosen, an attacker can overwrite various executables which could lead to escalation of the privileges when executed.

Tested Versions

Win-911 Enterprise V4.20.13

Product URLs

https://www.win911.com/

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 is a critical alerting platform which provides monitoring and alert configuration capability for SCADA/OT, HMI and control network environments. In supports various methods of alert configuration, routing and escalation designed to ensure safety of the environment.

By default, WIN-911 V4.20.13 is installed in “C:\Program Files (x86)\WIN-911 Software” directory and it allows “Everyone” group to have “Full” privilege over certain files in the directory which are executed with SYSTEM authority. This allows users in Everyone group to read, write or modify arbitrary files in the install directory resulting in privilege escalation in certain configuration.

CVE-2020-13539 - Privilege escalation via “WIN-911 Mobile Runtime” service

WIN-911 Mobile Runtime service allows any user on the system to replace binary located in program files as seen below to execute code with privilege of WIN-911 service user:

```
c:\program files (x86)\win-911 software\win-911 enterprise\mobile\WIN911.Notifier.Mobile.Runtime.exe
                                                                                    Everyone:F
                                                                                    BUILTIN\Administrators:F
                                                                                    NT AUTHORITY\Authenticated Users:(ID)
(special access:)
READ_CONTROL
FILE_READ_DATA
FILE_READ_EA
FILE_READ_ATTRIBUTES
```

CVE-2020-13540 - Privilege escalation via “WIN-911 Account Change Utility”

WIN-911 Account Change Utility is a program used to change WIN-911 service user which runs all of the associated windows services. Due to high level privilege required to execute this operation only an administrative level user can successfully reconfigure services. The executable, which enables this operation, can however be easily replaced by any user from “Everyone” group due to weak permissions applied on the application as seen below leading to privilege escalation when the application is used.

```
c:\Program Files (x86)\WIN-911 Software\ACU\WIN-911 Account Change Utility.exe
                                                                        BUILTIN\Administrators:(ID)F
Everyone:(ID)F
NT AUTHORITY\Authenticated Users:(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
```

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.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1141

NEXT REPORT TALOS-2020-1151