Talos Vulnerability Report

Advantech WebAccess/SCADA installation privilege escalation vulnerability

CVE NUMBER

CVE-2020-13551, CVE-2020-13552, CVE-2020-13553, CVE-2020-13554, CVE-2020-13555

Summary

Multiple exploitable local privilege elevation vulnerabilities exist in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. Depending on the vector chosen, an attacker can either replace binary or loaded modules to execute code with NT SYSTEM privilege.

Tested Versions

Advantech WebAccess/SCADA 9.0.1

Product URLs

https://www.advantech.com/industrial-automation/webaccess/webaccessscada

CVSSv3 Score

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

CWE

CWE-276 - Incorrect Default Permissions

Details

Advantech WebAccess/SCADA is an HTML5-based software package used to perform data visualization and supervisory controls over IoT/OT devices. It collects, parses and distributes data using MQTT.

CVE-2020-13551 - Privilege escalation via PostgreSQL executable

The service 'postgresql' starts with the following command:

```
"c:\postgresql\postgresql\bin\pg_ctl.exe" runservice -N "postgresql" -D "c:\postgresql\postgresql\data" -w -o "-F -p 5436"
```

Advantech WebAccess/SCADA PostgreSQL service allows any user on the system to replace binary located in the default installation folder, as seen below, to execute code with privilege of NT SYSTEM user:

```
c:\postgresql\postgresql\bin\pg_ctl.exe BUILTIN\Administrators:(ID)F
                                        NT AUTHORITY\SYSTEM:(ID)F
                                        BUILTIN\Users:(ID)R
                                        NT AUTHORITY\Authenticated Users:(ID)C
```

In addition, other components such as DLL libraries can be used to sideload code with high privilages as seen below:

```
C:\postgresql\postgresql\bin\libpq.dll BUILTIN\Administrators:(ID)F
                                       NT AUTHORITY\SYSTEM:(ID)F
                                       BUILTIN\Users:(ID)R
                                       NT AUTHORITY\Authenticated Users:(ID)C
```

Other libraries and binaries can also be used to exploit this vulnerablities so long they are loaded from the following location:

```
C:\postgresql\postgresql\bin\*
```

These can be, for example:

```
libiconv-2.dll
libpq.dll
libintl-8.dll
postgres.exe
```

CVE-2020-13552 - Privilege escalation via multiple service executables in installation folder of WebAccess

Advantech WebAccess/SCADA allows for any authenticated user on the system to replace binary located in default location as seen below to execute code with privilege of NT SYSTEM user. Depending on the vector chosen, the adversary can either replace libraries loaded from the folder of where service executables exist or replace service binary itself as detailed below.

The service 'SaaS-Composer_keep-alive' starts with the following command and have weak permissions:

```
C:\WebAccess\Node\WISE-PaaS_SaaS-Composer\SC-tool-keep-alive.exe BUILTIN\Administrators:(ID)F
                                                    BUILTIN\IIS_IUSRS:(ID)F
                                                    IIS APPPOOL\WaWebService_pool:(ID)F
                                                    IIS APPPOOL\Broadweb_pool:(ID)F
                                                    NT AUTHORITY\SYSTEM:(ID)F
                                                    BUILTIN\Users:(ID)R
                                                    NT AUTHORITY\Authenticated Users:(ID)C
```

The service 'WebAccessMongoDB' starts with the following command and have weak permissions:

```
C:\WebAccess\Node\mongodb\mongod64.exe BUILTIN\Administrators:F
                                       BUILTIN\IIS_IUSRS:F
                                       IIS APPPOOL\WaWebService_pool:F
                                       IIS APPPOOL\Broadweb_pool:F
                                       BUILTIN\Administrators:(ID)F
                                       BUILTIN\IIS_IUSRS:(ID)F
                                       IIS APPPOOL\WaWebService_pool:(ID)F
                                       IIS APPPOOL\Broadweb_pool:(ID)F
                                       NT AUTHORITY\SYSTEM:(ID)F
                                       BUILTIN\Users:(ID)R
                                       NT AUTHORITY\Authenticated Users:(ID)C
```

The service 'Dashboard' starts with the following command and have weak permissions:

```
C:\WebAccess\Node\WISE-PaaS_Dashboard\WISE-PaaS_Dashboard\bin\grafana-server.exe BUILTIN\Administrators:(ID)F
                                                    BUILTIN\IIS_IUSRS:(ID)F
                                                    IIS APPPOOL\WaWebService_pool:(ID)F
                                                    IIS APPPOOL\Broadweb_pool:(ID)F
                                                    NT AUTHORITY\SYSTEM:(ID)F
                                                    BUILTIN\Users:(ID)R
                                                    NT AUTHORITY\Authenticated Users:(ID)C
```

The service 'WISE-PaaS_SaaS-Composer' starts with the following command and have weak permissions:

```
C:\WebAccess\Node\WISE-PaaS_SaaS-Composer\SC-Management-Go.exe BUILTIN\Administrators:(ID)F
                                                    BUILTIN\IIS_IUSRS:(ID)F
                                                    IIS APPPOOL\WaWebService_pool:(ID)F
                                                    IIS APPPOOL\Broadweb_pool:(ID)F
                                                    NT AUTHORITY\SYSTEM:(ID)F
                                                    BUILTIN\Users:(ID)R
                                                    NT AUTHORITY\Authenticated Users:(ID)C
```

The service 'InfluxDB' starts with the following command and have weak permissions:

```
C:\WebAccess\Node\influxdb\InfluxDB.exe BUILTIN\Administrators:F
                                        BUILTIN\IIS_IUSRS:F
                                        IIS APPPOOL\WaWebService_pool:F
                                        IIS APPPOOL\Broadweb_pool:F
                                        BUILTIN\Administrators:(ID)F
                                        BUILTIN\IIS_IUSRS:(ID)F
                                        IIS APPPOOL\WaWebService_pool:(ID)F
                                        IIS APPPOOL\Broadweb_pool:(ID)F
                                        NT AUTHORITY\SYSTEM:(ID)F
                                        BUILTIN\Users:(ID)R
                                        NT AUTHORITY\Authenticated Users:(ID)C
C:\WebAccess\Node\influxdb\influxd.exe BUILTIN\Administrators:F
                                       BUILTIN\IIS_IUSRS:F
                                       IIS APPPOOL\WaWebService_pool:F
                                       IIS APPPOOL\Broadweb_pool:F
                                       BUILTIN\Administrators:(ID)F
                                       BUILTIN\IIS_IUSRS:(ID)F
                                       IIS APPPOOL\WaWebService_pool:(ID)F
                                       IIS APPPOOL\Broadweb_pool:(ID)F
                                       NT AUTHORITY\SYSTEM:(ID)F
                                       BUILTIN\Users:(ID)R
                                       NT AUTHORITY\Authenticated Users:(ID)C
```

CVE-2020-13553 - Privilege escalation via Node.js script source

By default Dashboard process, which starts as any user logged into system executes a series of Node.Js scripts to start additional application functionality. The execution tree used to run addition commands is as follows:

```
1) C:\Inetpub\wwwroot\broadweb\WADashboard\dashboard_start.exe process starts
2) C:\Inetpub\wwwroot\broadweb\WADashboard\WADashboard.exe C:\Inetpub\wwwroot\broadweb\WADashboard\startServerByServerConfig.js is executed
following successful start of dashboard_start.exe process
```

By default, "Everyone" group have Full permissions to write to the startServerByServerConfig.js file so appending simple JavaScript code to the source file will result in command execution with privilege of any user who starts dashboard_start.exe process:

```
const { exec } = require('child_process');
exec('whoami  > C:\\Users\\Public\\whoami.txt')
```

The permission on startServerByServerConfig.js file is set as follows:

```
C:\Inetpub\wwwroot\broadweb\WADashboard\startServerByServerConfig.js Everyone:F
                                                      BUILTIN\Administrators:(ID)F
                                                      BUILTIN\IIS_IUSRS:(ID)F
                                                      IIS APPPOOL\WaWebService_pool:(ID)F
                                                      IIS APPPOOL\Broadweb_pool:(ID)F
                                                      NT SERVICE\TrustedInstaller:(ID)F
                                                      NT AUTHORITY\SYSTEM:(ID)F
                                                      BUILTIN\Users:(ID)R
```

CVE-2020-13554 - webvrpcs Run Key Privilege Escalation

In the default configuration, the following registry keys, which reference binaries with weak permissions, can be abused by adversary to effectively 'backdoor' the installation files and escalate privileges when a new user logs in and uses the application:

```
Registry Key (x86): HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\webvrpcs
Registry Key (x64): HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\webvrpcs
Binary: C:\WebAccess\Node\webvrpcs.exe
Binary Permissions:
C:\WebAccess\Node\webvrpcs.exe BUILTIN\Administrators:F
                               BUILTIN\IIS_IUSRS:F
                               IIS APPPOOL\WaWebService_pool:F
                               IIS APPPOOL\Broadweb_pool:F
                               BUILTIN\Administrators:(ID)F
                               BUILTIN\IIS_IUSRS:(ID)F
                               IIS APPPOOL\WaWebService_pool:(ID)F
                               IIS APPPOOL\Broadweb_pool:(ID)F
                               NT AUTHORITY\SYSTEM:(ID)F
                               BUILTIN\Users:(ID)R
                               NT AUTHORITY\Authenticated Users:(ID)C
```

CVE-2020-13555 - COM Server Application Privilege Escalation

The following COM Class Identifiers (CLSID), installed by Advantech WebAccess/SCADA, reference LocalServer32 and InprocServer32 with weak privileges which can lead to privilege escalation when invoked by higher privilege users:

```
KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{139C94AB-8CB3-4D35-87AB-36C99B04C41D}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\ACProjDecrypt.dll
Permission:
C:\WebAccess\Node\ACProjDecrypt.dll BUILTIN\Administrators:F
                                    BUILTIN\IIS_IUSRS:F
                                    IIS APPPOOL\WaWebService_pool:F
                                    IIS APPPOOL\Broadweb_pool:F
                                    BUILTIN\Administrators:(ID)F
                                    BUILTIN\IIS_IUSRS:(ID)F
                                    IIS APPPOOL\WaWebService_pool:(ID)F
                                    IIS APPPOOL\Broadweb_pool:(ID)F
                                    NT AUTHORITY\SYSTEM:(ID)F
                                    BUILTIN\Users:(ID)R
                                    NT AUTHORITY\Authenticated Users:(ID)C
```

In addition, the following other COM servers were also observed as vulnerable:

```
KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{13486D51-4821-11D2-A494-3CB306C10000}\LocalServer32\LocalServer32
Binary: C:\WebAccess\Node\opcenum.exe

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{3703BA5D-7329-4E60-A1A5-AE7D6DF267C1}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\webdobj.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{3D8E72FD-4F8E-4495-83C2-C8D79AC8B25C}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\AspVCObj.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{4F545936-E755-4A5D-A0DC-B3614A55F501}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\WebSvcObj.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5484805F-03B3-4837-8C70-BD2705605CE4}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\AspVCObj.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{57CAF350-700F-4CC8-A02F-E1FFD8726A4E}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\bwenumtag.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7A4554E4-C2CE-41F7-8827-A45FA17DD5E3}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\AspVBObj.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7AB85B2C-FA45-4641-820C-EE8224CFD5E1}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\bwenumtag.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{81E463F4-2EDC-48D4-973E-816EB6AF67D8}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\BAExt.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{89D00354-B2EA-4755-915D-615D3962C7D7}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\AspVCObj.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{90CFA007-EE7B-4F22-96B9-D7B72A3DBEBB}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\EMSLib.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{94FC80D9-AEDB-4C18-9ECE-CAC8CE593704}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\BAExt.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{AAB22C2D-0E8F-4CCA-BB15-6581A1E12EC8}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\WebCliSocketX.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{ACE167D1-FAAA-4199-9159-71BB6D63D400}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\EMSLib.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{B0F68B04-7927-4264-9005-C9F30F67715F}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\BAExt.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BE8AF36A-93C9-4435-8858-2C59177ADA95}\LocalServer32\LocalServer32
Binary: C:\WebAccess\Node\wastchk.exe

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{CC8A7EE6-5425-4C97-9B36-C0B48F5F7EB4}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\EMSLib.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{F4204D29-B16E-4215-9862-4E50CA2BD519}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\webvobj.dll

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{F5842BD5-AFFC-41A2-BD6B-C1784B27CF27}\InprocServer32\InprocServer32
Binary: C:\WebAccess\Node\BAExt.dll
```

Timeline

2020-10-16 - Initial vendor contact
2020-10-20 - Vendor disclosure

2020-11-17 - 2nd follow up
2020-12-14 - 3rd follow up
2021-01-05 - 75 day follow up
2021-01-20 - 90 day final notice
2021-02-16 - Public release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.