Talos Vulnerability Report

TALOS-2020-1148

Moxa MXView series installation privilege escalation vulnerability

NOVEMBER 3, 2020

CVE NUMBER

CVE-2020-13537,CVE-2020-13536

SUMMARY

Multiple exploitable local privilege elevation vulnerabilities exist in the file system permissions of Moxa MXView series 3.1.8 installation. Depending on the vector chosen, an attacker can either add code to a script or replace a binary, both of which get executed by a service, thus executing arbitrary commands with System-level privileges.

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

Moxa MXView Series 3.1.8

PRODUCT URLS

MXView Series - https://www.moxa.com/en/products/industrial-network-infrastructure/network-management-software/mxview-series

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

Moxa's MXview network management software is a configuration management software for networking devices in industrial networks. It supports integrated platform management which can discover network devices installed in the subnet and allows for rapid configuration changes.

CVE-2020-13536 - Privilege escalation via Node.js script source

By default MXViewService, which starts as a NT SYSTEM authority user executes a series of Node.Js scripts to start additional application functionality. The execution tree used to run addition commands is as follows:

```
services.exe -> MXViewServiceControl.exe -> MXView.exe -> MXViewCore.exe -> node.exe
```

The final command which executes `node.exe` is started as follows:

```
node.exe "C:\Users\[user]\AppData\Roaming\moxa\mxview\MXview-gateway\dist\bundle.js" --use-strict -vv -d 127.0.0.1 -p 4430 -h [xxxx] --
dbpass=[xxxx] -c "C:\Users\[user]\AppData\Roaming\moxa\mxview\MXview-gateway\config\gateway.ini"  --fileLock=gatewaylock
```

By default, “Users” group have Full permissions to write to the `bundle.js` file so appending simple JavaScript code to the source file will result in command execution with NT SYSTEM privilage:

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

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

```
C:\Users\[user]\AppData\Roaming\moxa\mxview\MXview-gateway\dist\bundle.js
                                                                     BUILTIN\Users:(ID)F
                                                                     NT AUTHORITY\SYSTEM:(ID)F
                                                                     BUILTIN\Administrators:(ID)F
```

The following files can also be abused to trigger this vulnerablity:

```
C:\Users\[user]\AppData\Roaming\moxa\mxview\mxview-gateway\utils\mosquitto_start.js
                                                                                BUILTIN\Users:(ID)F
                                                                                NT AUTHORITY\SYSTEM:(ID)F
                                                                                BUILTIN\Administrators:(ID)F
```

CVE-2020-13537 - Privilege escalation via mosquitto executable

By default MXViewService, which starts as a NT SYSTEM authority user executes a series of Node.Js scripts to start additional application functionality and among them the mosquitto executable is also run. The execution tree used to run addition commands is as follows:

```
services.exe -> MXViewServiceControl.exe -> MXView.exe -> MXViewCore.exe -> node.exe -> mosquitto.exe
```

Eventually, `node.exe` executes `mosquitto.exe` as follows thus leading to privilege escalation if binary is replaced by an aversary:

```
./bin/mosquitto/mosquitto.exe -p 8883 -c ./mosquitto.conf
```

By default, “Users” group have Full permissions to write to the `mosquitto.exe` file so replacement of the executable will lead to command execution with NT SYSTEM privilage:

```
C:\Users\[user]\AppData\Roaming\moxa\mxview\mxview-gateway\bin\mosquitto\mosquitto.exe
                                                                                   BUILTIN\Users:(ID)F
                                                                                   NT AUTHORITY\SYSTEM:(ID)F
                                                                                   BUILTIN\Administrators:(ID)F
```

In addition, the following other folders with various executables and dll files, also invoked by MXViewService can be replaced using similar method to achieve privilage escalation:

```
C:\Users\[user]\AppData\Roaming\moxa\mxview\mxview-gateway\bin\mosquitto BUILTIN\Users:(OI)(CI)(ID)F

NT AUTHORITY\SYSTEM:(OI)(CI)(ID)F

BUILTIN\Administrators:(OI)(CI)(ID)F
C:\Users\[user]\AppData\Roaming\moxa\mxview\mxview-gateway\bin\pgsql BUILTIN\Users:(OI)(CI)(ID)F
                                                                                                                                          NT
AUTHORITY\SYSTEM:(OI)(CI)(ID)F

BUILTIN\Administrators:(OI)(CI)(ID)F
C:\Users\[user]\AppData\Roaming\moxa\mxview\mxview-gateway\bin\protobuf BUILTIN\Users:(OI)(CI)(ID)F

NT AUTHORITY\SYSTEM:(OI)(CI)(ID)F

BUILTIN\Administrators:(OI)(CI)(ID)F
```

TIMELINE

2020-09-01 - Vendor Disclosure
2020-11-04 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

NEXT REPORT

TALOS-2020-1086

TALOS-2020-1157