Talos Vulnerability Report

TALOS-2021-1403

Moxa MXView Series Web Application information disclosure vulnerability

FEBRUARY 11, 2022

CVE NUMBER

CVE-2021-40392

Summary

An information disclosure vulnerability exists in the Web Application functionality of Moxa MXView Series 3.2.4. Network sniffing can lead to a disclosure of sensitive information. An attacker can sniff network traffic to exploit this vulnerability.

Tested Versions

Moxa MXView Series 3.2.4

Product URLs

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

CVSSv3 Score

5.3 - CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N

CWE

CWE-319 - Cleartext Transmission of Sensitive Information

Details

Moxa's MXView network management software is designed for configuring, monitoring and diagnosing networking devices in industrial networks. MXView provides an integrated management platform that can discover networking devices and SNMP/IP devices installed on subnets. All selected network components can be managed via a web browser from both local and remote sites—anytime and anywhere.

The default installation of the MXView web application is configured to transmit credentials in cleartext. Neither the credentials nor the communication channel are encrypted, requiring administrators to explicitly disable unencrypted protocols.

Exploit Proof of Concept

The following is an example of an HTTP POST request that is sent with unencrypted credentials when logging in to the application:

```
POST /login HTTP/1.1
Host: <IP>
Content-Type: application/json
Content-Length: 38
Connection: close

{"username":"admin","password":"moxa"}
```

Mitigation

Unencrypted network communication may be disabled by:

- unchecking the "Enable HTTP" option during installation
- checking the "Disable HTTP Port" option in the MXView application
- unchecking the "Enable HTTP Port" option in the MXView Configuration Tool
- changing the "Web console protocol" settings in the web application (Preferences > Advanced > Management Interface > change HTTP to HTTPS)

Timeline

2021-10-20 - Vendor disclosure
2022-02-11 - Public Release

CREDIT

Discovered by Patrick DeSantis of Cisco Talos.
