Talos Vulnerability Report

TALOS-2021-1401

Moxa MXView Series Web Application authentication bypass vulnerability

FEBRUARY 11, 2022

CVE NUMBER

CVE-2021-40390

Summary

An authentication bypass vulnerability exists in the Web Application functionality of Moxa MXView Series 3.2.4. A specially-crafted HTTP request can lead to unauthorized access. An attacker can send an HTTP request to trigger 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

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

CWE

CWE-798 - Use of Hard-coded Credentials

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 MXview adds an undocumented service listening on port 4430 which accepts authentication using admin:moxa with no obvious or documented way to change or disable this access. Changing the admin user's password via a different service, such as the web application on ports 80/443, does not change the password for the service on port 4430 (referred to as the "polling engine port" during installation). There does not appear to be a "change password" function for this service.

Logging in to this service with these credentials provides administrator access to the MXview application's functionality.

Timeline

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

CREDIT

Discovered by Patrick DeSantis of Cisco Talos.

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.