ICS-CERT REPORT

Rahul Jayakrishnan GTID:903281837

Allen Bradley Micrologix 1100 Family

1.

Model Number:1766-L32BWA, Series A and B, Version 16.00 and prior versions

Vulnerability discovered:PREDICTABLE VALUE RANGE FROM PREVIOUS VALUES

Description: This vulnerability allows attackers predict numbers from previous values as the initial TCP sequence numbers generated are not sufficiently random. This could allow attackers to spoof TCP connections associated with the PLC.

2.

Model Number:1766-L32BWA, Series A and B, Version 16.00 and prior versions

Vulnerability discovered:REUSING A NONCE, KEY PAIR IN ENCRYPTION

Description: The reuse of nonces exposes the device to potential replay attacks until the nonce is changed

3.

Model Number:1766-L32BWA, Series A and B, Version 16.00 and prior versions

Vulnerability discovered:INFORMATION EXPOSURE

Description: Attackers may gain unauthorised access to user credentials as they are sent to the server using HTTP GET method

4.

Model Number:1766-L32BWA, Series A and B, Version 16.00 and prior versions

Vulnerability discovered:IMPROPER RESTRICTION OF EXCESSIVE AUTHENTICATION ATTEMPTS

Description: The device is vulnerable to brute force attacks as there is no penalty for repeatedly entering the wrong password

5.

Model Number:1766-L32BWA, Series A and B, Version 16.00 and prior versions

Vulnerability discovered:WEAK PASSWORD REQUIREMENTS

Description: small maximum password size is use resulting in weak passwords to protect devices that are affected.