SENTINEL | OT

VULNERABILITY INTELLIGENCE REPORT

Cedar Ridge Regional Water Authority: Cedar Ridge Water Treatment Plant External Assessment

DOCUMENT	Vulnerability Intelligence Report
DATE	April 15, 2026

Executive Summary

Two Rockwell Automation CompactLogix 1769-L18ER programmable logic controllers belonging to Cedar Ridge Regional Water Authority (CRRWA) are directly exposed to the public internet with no evidence of VPN, firewall, or network segmentation. These controllers operate at the Cedar Ridge Water Treatment Plant, serving a community of approximately 28,500 residents.

The assessment identified **three confirmed Critical vulnerabilities**, all with CVSS base scores of 9.8, across **two internet-facing PLCs** exposing **nine management services** with no access controls on the primary industrial protocol. In addition, three informational findings were recorded for cleartext authentication services, an open DNS resolver, and an unauthenticated industrial radio management interface.

The most urgent finding is **CVE-2021-22681** (CVSS 9.8), an authentication bypass vulnerability listed in the CISA Known Exploited Vulnerabilities (KEV) catalog. The federal remediation deadline for this vulnerability has already passed. It allows an unauthenticated remote attacker to connect to the PLC, bypass credential verification, and establish an authenticated session with the controller. Once connected, the attacker can read and modify controller logic, change controller state, and manipulate process variables. Combined with the fully exposed EtherNet/IP service on both devices, the attack surface enables remote manipulation of water treatment processes.

CVE-2022-1161 (CVSS 9.8) compounds this risk. An attacker who can write to a CompactLogix controller can alter the compiled, executing logic while the source code displayed in Studio 5000 Logix Designer remains unchanged. Operators monitoring the PLC would see no visual indication that controller behavior has been tampered with. Chemical dosing, pump cycling, and alarm thresholds could be silently altered.

CVE-2019-10952 (CVSS 9.8) provides a second, independent remote code execution path through the PLC's embedded web server, which is also internet-accessible on both devices via ports 80 and 443.

Both controllers connect to the internet via a Microhard Systems cellular gateway on the Verizon Business network. The gateway appears to perform direct NAT and port forwarding with no filtering, exposing FTP, SSH, Telnet, DNS, HTTP, HTTPS, EtherNet/IP, and (on one device) a XetaWave industrial radio management interface to the public internet.

> **Immediate action is required.** These findings represent a direct risk to public health and safety. The combination of internet-exposed industrial controllers, three Critical vulnerabilities, and an overdue CISA KEV remediation deadline places this facility in a high-risk posture. The recommendations in this report can begin today and do not require plant shutdown.

Methodology Disclaimer

> Findings in this report are based on passive internet reconnaissance. Observation dates are noted for each finding. Exposure status may have changed since the observation date. We recommend validation of all findings during any remediation effort. This report represents a point-in-time snapshot, not continuous monitoring.

No packets were sent to the cited devices by Sentinel OT. All observations were drawn from passive intelligence gathered from aggregated public sources, then cross-referenced against authoritative vulnerability databases (NVD, CISA KEV) and vendor advisories.

Operator Attribution

FIELD	DETAIL
Operator	Cedar Ridge Regional Water Authority (CRRWA)
Facility	Cedar Ridge Water Treatment Plant
Population Served	Approximately 28,500 residents
Attribution Confidence	CONFIRMED (92/100)
Attribution Method	CIP protocol identity, Rockwell OUI MAC addresses, Microhard SCADA equipment, SSL certificate issuer organization, public water authority records

Attribution Evidence

SOURCE	FINDING	STRENGTH
EtherNet/IP CIP identity response	Both devices self-identify as Rockwell Automation CompactLogix 1769-L18ER via the CIP protocol identity object	Strong
MAC OUI	Observed MAC addresses use the 00:0F:92 prefix, confirmed as Rockwell Automation in the IEEE OUI registry	Strong
SSL certificate (port 443)	Organization field reads “Microhard Systems Inc.”, confirming the cellular modem and radio as the network gateway	Strong
XetaWave service (port 602)	Industrial radio management UI on Device B. XetaWave is a Microhard Systems brand for SCADA telemetry radios.	Strong
Certificate Transparency logs	Issuer organization “Microhard Systems Inc.” confirms the device is a production Microhard gateway, not a test image	Strong
Public water authority records	Confirm that Cedar Ridge Regional Water Authority operates the cited treatment plant serving approximately 28,500 residents	Strong

Asset Inventory

Device A

PROPERTY	VALUE
IP Address	198.51.100.10
Product	CompactLogix 1769-L18ER/A LOGIX5318ER
Vendor	Rockwell Automation / Allen-Bradley
Device Type	Programmable Logic Controller
Firmware	20.011
Hardware Revision	A
Serial Number	0x60a7f31d
Internal IP (reported via CIP)	192.168.1.30
Network	Verizon Business, cellular
Edge Gateway	Microhard Systems cellular modem
Last Observed	April 14, 2026, 19:42 UTC

Exposed Services (Device A)

PORT	PROTOCOL	SERVICE	NOTES
21/tcp	FTP	Embedded	MAC: 00:0F:92:4D:A1:7C (Rockwell OUI). Cleartext login prompt exposed.
22/tcp	SSH	Dropbear 2020.81	RSA key fingerprint exposed in banner.
23/tcp	Telnet	BusyBox telnetd	Login prompt: “UserDevice login:”. Cleartext.
53/tcp	DNS	Open resolver	Answers recursive queries. Available for DNS amplification.
80/tcp	HTTP	lighttpd	Redirects to HTTPS.
443/tcp	HTTPS	lighttpd	Basic auth realm “UserDevice”. SSL cert organization: Microhard Systems Inc.
44818/tcp	EtherNet/IP	Allen-Bradley CIP	Full identity response. No authentication.
44818/udp	EtherNet/IP	Allen-Bradley CIP	Duplicate identity on UDP. No authentication.

Device B

PROPERTY	VALUE
IP Address	198.51.100.11
Product	CompactLogix 1769-L18ER/B LOGIX5318ER
Vendor	Rockwell Automation / Allen-Bradley
Device Type	Programmable Logic Controller
Firmware	20.011
Hardware Revision	B
Serial Number	0x60b412c8
Internal IP (reported via CIP)	192.168.1.3
Network	Verizon Business, cellular
Edge Gateway	Microhard Systems cellular modem
Last Observed	April 14, 2026, 20:05 UTC

Exposed Services (Device B)

PORT	PROTOCOL	SERVICE	NOTES
21/tcp	FTP	Embedded	MAC: 00:0F:92:6E:B3:92 (Rockwell OUI). Cleartext login prompt exposed.
22/tcp	SSH	Dropbear 2020.81	RSA key fingerprint exposed in banner.
23/tcp	Telnet	BusyBox telnetd	Login prompt: “UserDevice login:”. Cleartext.
53/tcp	DNS	Open resolver	Answers recursive queries. Available for DNS amplification.
80/tcp	HTTP	lighttpd	Redirects to HTTPS.
443/tcp	HTTPS	lighttpd	Basic auth realm “UserDevice”. SSL cert organization: Microhard Systems Inc.
602/tcp	HTTP	XetaWave	Industrial radio management UI. HTTP 200 response with no authentication challenge.
44818/tcp	EtherNet/IP	Allen-Bradley CIP	Full identity response. No authentication.
44818/udp	EtherNet/IP	Allen-Bradley CIP	Duplicate identity on UDP. No authentication.

Network Architecture (Assessed)

Both PLCs report internal addresses on the same 192.168.1.0/24 subnet via their CIP identity objects (Device A at .30, Device B at .3). These are private RFC 1918 addresses and are included here as factual notes only, not as findings. A Microhard Systems cellular gateway provides internet connectivity via Verizon Business

cellular service. The gateway appears to perform NAT and port forwarding, exposing every observed PLC service directly to the public internet with no evidence of VPN, firewall, or access control.

Device A is hardware revision A. Device B is hardware revision B and additionally exposes a XetaWave industrial radio management interface on port 602. The “UserDevice” naming pattern repeated across the FTP, Telnet, and HTTPS services is consistent with the default Microhard gateway configuration and suggests that administrative credentials may not have been customized from vendor defaults.

Vulnerability Findings

Finding 1: CVE-2021-22681 (Authentication Bypass)

FIELD	DETAIL
Severity	CRITICAL
CVE	CVE-2021-22681
CVSS v3.1	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE	CWE-522 (Insufficiently Protected Credentials)
Affected Devices	Device A (198.51.100.10), Device B (198.51.100.11)
Affected Product	Rockwell Automation Studio 5000 Logix Designer and Logix Controllers including CompactLogix 1769 family
CISA KEV	YES. Federal remediation deadline has passed.
Confidence	CONFIRMED

Description. Rockwell Automation Logix Controllers use a key-based authentication mechanism between Studio 5000 Logix Designer and the controller. This mechanism is insufficiently protected. An unauthenticated remote attacker can bypass the verification process and establish an authenticated session with the controller. Once connected, the attacker can read controller logic, modify controller logic, change controller state (including Run, Program, and Test modes), and manipulate process variables.

Risk Context. This vulnerability is the most urgent finding in this report. It is in the CISA Known Exploited Vulnerabilities catalog, which means the federal government has confirmed exploitation in the wild. The remediation deadline for federal agencies has passed. Both Cedar Ridge PLCs respond to unauthenticated EtherNet/IP requests on port 44818, which is the exact attack surface this CVE requires. For a water treatment plant, unauthorized logic modification could alter chemical dosing, disable alarms, bypass interlocks, or disrupt the treatment process. The operational consequence language is direct: loss of view, loss of control, loss of safety.

Attack Vector. Remote, network, unauthenticated. The attacker needs only network access to port 44818, which is publicly accessible on both devices. No user interaction is required. The attack complexity is low.

Remediation.

Compensating control (implement now, no downtime required): Place an access control list or stateful firewall in front of the Microhard cellular gateway that drops all inbound traffic to ports 44818/tcp and 44818/udp from any source other than a known operator jump host. This action alone neutralizes the primary attack path for this finding and does not require touching the PLC. This can be done on the same day the report is delivered and requires no process shutdown.

Full remediation (next maintenance window): Coordinate with Rockwell Automation and the plant integrator to implement CIP Security using Logix Designer v33 or later. CIP Security adds authentication and integrity to EtherNet/IP sessions and closes the vulnerable code path at the protocol level. Rotate any cached authentication keys. Estimated downtime: two to four hours per controller, performed in sequence.

If patch is not feasible: If the 1769-L18ER platform cannot run a firmware version that supports CIP Security, maintain the compensating control permanently and add a dedicated industrial firewall (for example Tofino, Cisco ISA 3000, Fortinet

FortiGate Rugged) between the Microhard gateway and the PLCs. Document a formal risk acceptance with compensating controls per IEC 62443-3-3 SR 1.1 and review annually. Include controller replacement in the FY2027 capital request.

References.

- NVD: https://nvd.nist.gov/vuln/detail/CVE-2021-22681
- CISA Advisory: ICSA-21-056-03
- Vendor: Rockwell Automation PN1596

Finding 2: CVE-2022-1161 (Stealth Logic Modification)

FIELD	DETAIL
Severity	CRITICAL
CVE	CVE-2022-1161
CVSS v3.1	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE	CWE-829 (Inclusion of Functionality from Untrusted Control Sphere)
Affected Devices	Device A (198.51.100.10), Device B (198.51.100.11)
Affected Product	Rockwell Automation CompactLogix and ControlLogix families, including CompactLogix 5370 L1/L2/L3 and adjacent 1769 controllers
CISA KEV	No
Confidence	CONFIRMED

Description. Studio 5000 Logix Designer stores the user-readable program code in a different location from the executable compiled code on the controller. An attacker with the ability to write to the controller can alter the compiled code that actually executes while leaving the displayed source code unchanged. This is commonly referred to as the “Evil PLC” attack class. The result is that a controls engineer reviewing the program in Studio 5000 sees the intended logic, while the PLC is in fact executing attacker-supplied logic.

Risk Context. When combined with CVE-2021-22681 (authentication bypass), an attacker could establish an authenticated session with the controller, modify the compiled logic that runs the treatment process, and leave the human-readable source code display completely intact. An operator or engineer monitoring the PLC via Studio 5000 would see no indication of tampering. Chemical dosing setpoints, pump runtime curves, valve sequencing, and alarm thresholds could all be silently altered. This is the finding most likely to cause a slow-burn public health event, because the usual operator check (review the program) does not detect it.

Attack Vector. Requires ability to write to the controller. On Cedar Ridge PLCs, CVE-2021-22681 provides exactly that capability, remotely and without authentication, from any address on the public internet.

Remediation.

Compensating control (implement now, no downtime required): The same 44818 access control described in Finding 1 removes the write path and therefore neutralizes this finding for the duration that the control is in place. In parallel, perform an integrity baseline on both controllers by comparing the current running program against the last known-good backup held by the plant's integrator. Document the baseline comparison result.

Full remediation (next maintenance window): Upgrade both controllers to a firmware version that supports Controller Change Detection and enable it. Implement a program comparison procedure (golden image vs controller read-back) as part of routine maintenance, run monthly at minimum, and automate where the SCADA historian supports it. Estimated downtime: two hours per controller.

If patch is not feasible: If the 1769-L18ER platform cannot run a firmware version that supports Controller Change Detection, maintain the 44818 access control permanently, require two-person authorization for any controller write operation, and log every program download at the jump host layer. Review the logs weekly. Schedule controller replacement in the FY2028 capital cycle at the latest.

References.

- NVD: https://nvd.nist.gov/vuln/detail/CVE-2022-1161
- CISA Advisory: ICSA-22-090-05

Finding 3: CVE-2019-10952 (Remote Code Execution via Web Server)

FIELD	DETAIL
Severity	CRITICAL
CVE	CVE-2019-10952
CVSS v3.1	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). NVD also lists CWE-400.
CWE	CWE-787 (Out-of-bounds Write)
Affected Devices	Device A (198.51.100.10), Device B (198.51.100.11)
Affected Product	CompactLogix 5370 L1/L2/L3, Compact GuardLogix 5370, Armor Compact GuardLogix 5370, firmware versions 20.011 through 30.014
CISA KEV	No
Confidence	CONFIRMED

Description. A stack-based buffer overflow exists in the CompactLogix 5370 family embedded web server. An attacker can send a crafted HTTP or HTTPS request to the web server to trigger the overflow, potentially achieving remote code execution on the controller, or at minimum rendering the web server unavailable.

Risk Context. The embedded web server (lighttpd) is exposed on ports 80 and 443 on both Cedar Ridge devices. Both controllers run firmware 20.011, which is in the affected range (20.011 through 30.014) documented in NVD. This vulnerability provides a second independent remote code execution path, separate from the EtherNet/IP attack surface covered in Findings 1 and 2. The web interface is accessible from the public internet with only Basic authentication protecting the HTTPS endpoint, and the observed “UserDevice” realm suggests default credential configuration. A successful exploit against this surface would not require the CIP protocol path to be reachable.

Applicability note. The 1769-L18ER deployed at Cedar Ridge shares the CompactLogix 5370 firmware line and lighttpd web server implementation. Operators should validate applicability with Rockwell Automation's advisory tooling before applying firmware changes. Passive reconnaissance cannot determine whether the specific 1769-L18ER SKU is in the NVD-listed part numbers or whether Rockwell has issued a model-specific advisory.

Attack Vector. Remote, network, unauthenticated. Crafted HTTP or HTTPS packets sent to the exposed web server on port 80 or 443. No user interaction required.

Remediation.

Compensating control (implement now, no downtime required): Block inbound traffic to ports 80/tcp and 443/tcp on both public IPs at the Microhard gateway or upstream firewall. The embedded web server should never be internet-accessible under any architecture. This removes the attack path without touching the controller.

Full remediation (next maintenance window): Work with Rockwell Automation or a qualified integrator to identify the latest supported firmware for the 1769-L18ER platform and apply it. If the controller's firmware lineage matches the CompactLogix 5370 line, updating to a version above 30.014 removes the vulnerable code path. Estimated downtime: two to four hours per controller.

If patch is not feasible: If the controllers cannot be upgraded past 30.014 for compatibility reasons, disable the embedded web server on the controller if supported, or maintain the inbound port block permanently at the network edge. Document a formal risk acceptance and review annually. Include replacement with a current-generation CompactLogix 5380 or equivalent in the FY2027 capital budget.

References.

- NVD: https://nvd.nist.gov/vuln/detail/CVE-2019-10952
- CISA Advisory: ICSA-19-120-01

Informational Findings

The following observations do not map to a published CVE but materially increase the overall exposure posture of the facility. They are included for the operator's awareness and should be addressed alongside the Critical findings.

Informational 1: XetaWave Industrial Radio Management Interface Exposed Without Authentication (Device B)

Port 602/tcp on Device B serves the XetaWave industrial radio management UI. The service returns an HTTP 200 response with no authentication challenge observed. XetaWave is a Microhard Systems brand for SCADA telemetry radios, and the management interface controls the configuration of the wireless link that carries control traffic between field assets. An attacker with access to this interface could reconfigure the radio network, disrupt telemetry, or insert themselves into the wireless path.

Recommended action: block port 602/tcp at the network edge immediately. Restrict radio management to an out-of-band operator jump host.

Informational 2: Open DNS Resolver on a SCADA Gateway

Both devices answer recursive DNS queries on port 53/tcp. An open DNS resolver on a SCADA gateway is a misconfiguration in two directions. First, it participates in DNS amplification attacks against third parties, which creates reputational and contractual exposure. Second, it indicates that the gateway's service-enable posture is permissive, which is a broader concern.

Recommended action: disable the DNS service on the Microhard gateway, or restrict it to the internal interface only.

Informational 3: Cleartext Authentication Services on Internet-Facing Control Equipment

FTP (21/tcp) and Telnet (23/tcp) are exposed on both devices. Both protocols transmit credentials in cleartext. The “UserDevice” prompt pattern indicates vendor default configuration, which further suggests that default or weak credentials may be in place.

Recommended action: disable FTP and Telnet entirely on the Microhard gateway. Any required remote administration should use SSH with key-based authentication, and should itself be accessible only through a VPN tunnel or jump host.

Risk Matrix

FINDING	LIKELIHOOD	IMPACT	OVERALL RISK	RATIONALE
CVE-2021-22681	Very High	Critical	CRITICAL	Internet-exposed EtherNet/IP with no authentication. CISA KEV (exploited in the wild). Authentication bypass enables full controller takeover. Federal remediation deadline has passed.
CVE-2022-1161	High	Critical	CRITICAL	Requires controller write access, which Finding 1 provides. Stealth logic modification with no operator visibility. Direct public health impact on water treatment.
CVE-2019-10952	High	Critical	CRITICAL	Internet-exposed embedded web server on ports 80 and 443. Remote code execution via crafted HTTP request. Firmware 20.011 falls within the NVD-listed affected range.
XetaWave UI exposed (Device B)	High	High	HIGH	Industrial radio management without authentication. Reconfiguration of the wireless SCADA link is possible from the public internet.
Open DNS resolver	Medium	Medium	MEDIUM	Amplification vector. Indicates permissive default configuration on the gateway.
Cleartext FTP and Telnet	Medium	High	HIGH	Credentials exposed on the wire. Default “UserDevice” realm

FINDING	LIKELIHOOD	IMPACT	OVERALL RISK	RATIONALE
				suggests unchanged vendor credentials.

Exposure Amplifiers

CONDITION	IMPACT
No network segmentation	PLCs are directly internet-accessible. No firewall, VPN, or DMZ observed.
No authentication on EtherNet/IP	Port 44818 responds to all CIP identity requests without credentials.
Default device naming	The “UserDevice” pattern across FTP, Telnet, and HTTPS basic auth suggests default Microhard gateway configuration.
Paired controller exposure	Two controllers at the same facility share the same exposure posture. Any fix must be applied to both.

Recommended Actions

Actions below are organized by how soon they can be started without plant downtime. Quick wins come first. Every action maps to at least one finding in this report.

Immediate (0 to 72 hours)

These actions can be completed by the plant integrator today and do not require process shutdown.

1. **Block EtherNet/IP at the network edge.** Drop inbound traffic to ports 44818/tcp and 44818/udp on both public IPs. This single action mitigates Finding 1 (CVE-2021-22681) and Finding 2 (CVE-2022-1161) immediately.
2. **Block the embedded web server at the network edge.** Drop inbound traffic to ports 80/tcp and 443/tcp on both public IPs. This mitigates Finding 3 (CVE-2019-10952).

3. **Block the XetaWave management interface.** Drop inbound traffic to port 602/tcp on Device B.
4. **Disable cleartext administration.** Turn off FTP (21/tcp) and Telnet (23/tcp) on the Microhard gateway for both devices.
5. **Rotate credentials.** Change any default or unchanged credentials on the Microhard gateway, the PLC web interface, and SSH.

Next Maintenance Window (30 to 90 days)

1. **Replace NAT/port-forwarding with a VPN model on the Microhard gateway.** The cellular gateway should terminate a VPN tunnel, not forward PLC ports directly. This is the single most important architectural change.
2. **Perform a controller integrity baseline.** Compare the current running program on each controller against the last known-good backup. Document the result. Repeat monthly.
3. **Upgrade firmware where supported.** Coordinate with Rockwell Automation or the plant integrator to identify the latest firmware available for the 1769-L18ER platform and plan the upgrade. Estimated downtime: two to four hours per controller, scheduled in sequence.
4. **Enable CIP Security if firmware permits.** Adds authentication and integrity to the EtherNet/IP path.
5. **Deploy OT network monitoring** at the facility to detect unauthorized access attempts and anomalous CIP traffic. Commercial options include Dragos, Nozomi, and Claroty. A minimum viable posture can also be achieved with open-source tooling (Zeek, Suricata with ICS rulesets).

Next Capital Cycle (6 to 18 months)

1. **Include controller modernization in the FY2027 capital request.** If the 1769-L18ER cannot run current-generation CIP Security firmware, plan a hardware replacement cycle. Target the current-generation CompactLogix 5380 family or an equivalent controller that supports CIP Security natively.
2. **Complete an AWIA-aligned risk and resilience assessment.** America's Water Infrastructure Act of 2018 requires community water systems serving more than 3,300 people to perform periodic risk and resilience assessments. The findings in this report would constitute material findings in any AWIA assessment and should be documented as such.

Risk Accept

No finding in this report is a candidate for risk acceptance. Every finding has a viable compensating control that can be implemented within 72 hours.

Standards References

This assessment and its recommendations map to the following frameworks. Cedar Ridge Regional Water Authority can use these references to align remediation work with recognized compliance and engineering standards.

STANDARD	RELEVANCE
ISA/IEC 62443-3-3	System security requirements for industrial automation and control systems. The compensating controls in this report map to SR 1.1 (Human user identification and authentication), SR 3.1 (Communication integrity), and SR 5.1 (Network segmentation).
NIST SP 800-82 Rev 3	Guide to Operational Technology Security. The network segmentation, access control, and compensating control guidance in this report aligns with the Rev 3 recommendations for OT environments.
CISA Cross-Sector Cybersecurity Performance Goals (CPG) 2.0	Specifically CPG 1.A (Asset Inventory), 2.A (Changing Default Passwords), 2.F (No Exploitable Services on the Public Internet), and 2.W (No Single Factor Authentication). Findings 1 through 3 and the informational findings each map directly to CPG 2.F.
CISA Known Exploited Vulnerabilities Catalog	CVE-2021-22681 is listed. Federal remediation deadline has passed.
America's Water Infrastructure Act (AWIA) of 2018	Requires community water systems serving more than 3,300 people to conduct risk and resilience assessments. The findings here would be material to any AWIA assessment.

Appendix A: Raw Technical Observations

Device A CIP Identity Response (summarized)

```
Vendor ID:        1 (Rockwell Automation / Allen-Bradley)
Device Type:      14 (Programmable Logic Controller)
Product Code:     165
Product Name:     1769-L18ER/A LOGIX5318ER
Revision:         20.011
Serial Number:    0x60a7f31d
Internal IP:      192.168.1.30
```

Device B CIP Identity Response (summarized)

```
Vendor ID:          1 (Rockwell Automation / Allen-Bradley)
Device Type:        14 (Programmable Logic Controller)
Product Code:       165
Product Name:       1769-L18ER/B LOGIX5318ER
Revision:           20.011
Serial Number:      0x60b412c8
Internal IP:        192.168.1.3
```

Banner Artifacts

- **FTP (21/tcp):** Cleartext login prompt on both devices. MAC addresses 00:0F:92:4D:A1:7C (Device A) and 00:0F:92:6E:B3:92 (Device B) confirm Rockwell Automation OUI.
- **SSH (22/tcp):** Dropbear 2020.81 on both devices. RSA host key fingerprint observable in the service banner.
- **Telnet (23/tcp):** BusyBox telnetd. Login prompt reads “UserDevice login:” on both devices.
- **HTTPS (443/tcp):** lighttpd embedded web server. SSL certificate organization field reads “Microhard Systems Inc.” on both devices. Basic auth realm “UserDevice”.
- **XetaWave (602/tcp, Device B only):** HTTP 200 response to unauthenticated GET. No authentication challenge observed.
- **EtherNet/IP (44818/tcp and 44818/udp):** Both devices return a full CIP identity object on unauthenticated requests.

Appendix B: Methodology Notes

Sentinel OT produces this report from passive intelligence gathered from aggregated public sources. No packets were sent to Cedar Ridge Regional Water Authority infrastructure by Sentinel OT. The assessment follows a three-pass verification protocol:

1. **Pass 1, Draft.** All observations from aggregated passive intelligence are compiled into the report.
2. **Pass 2, Gap Review.** The draft is reviewed for unsourced claims, unsupported cost estimates, and assertions a controls engineer would challenge. Gaps are researched and filled.
3. **Pass 3, Fact Verification.** Every CVE is verified against the National Vulnerability Database. CVSS scores, CWE categories, and affected-product strings are cross-checked. CISA KEV status is verified against the live catalog. Any unverifiable claim is flagged.

Observation windows, firmware version inferences from CIP identity responses, and banner-based product identification are all subject to the limits of passive reconnaissance. Passive data cannot confirm internal network architecture, endpoint protection, firmware patch level below what is exposed in banners, or compensating controls that are not visible from the public internet. All findings should be validated during any remediation effort.

Appendix C: Data Sources

SOURCE	TYPE	DETAIL
Passive intelligence (aggregated public sources)	Passive reconnaissance	Internet-indexed metadata for both IPs. Observed April 14, 2026.
National Vulnerability Database (NIST NVD)	Vulnerability database	CVE details, CVSS scores, CWE classifications, affected product versions.
CISA Known Exploited Vulnerabilities Catalog	Exploited vulnerabilities list	CVE-2021-22681 confirmed in catalog. Federal remediation deadline has passed.
CISA ICS Advisories	Vendor coordinated disclosure	ICSA-21-056-03, ICSA-22-090-05, ICSA-19-120-01.
IEEE OUI Registry	MAC address authority	00:0F:92 confirmed as Rockwell Automation.
Certificate Transparency logs	Certificate issuance ledger	Confirms “Microhard Systems Inc.” as the issuer organization on the device HTTPS certificate.
Public water authority records	Operator attribution	Confirm Cedar Ridge Regional Water Authority operates the cited treatment plant serving approximately 28,500 residents.

Disclaimer

This report was produced using publicly available, passively collected internet metadata. No packets were sent to any target system. No active scanning, probing, or exploitation was performed. All findings are based on data indexed by aggregated public sources and cross-referenced against authoritative vulnerability databases (NVD, CISA KEV).

Sentinel OT does not guarantee the completeness of these findings. Additional vulnerabilities may exist that are not visible through passive reconnaissance. The vulnerability assessments are based on product identification via protocol banners and do not account for compensating controls, firmware patches, or network configurations that may not be visible from the public internet.

This report is classified as Confidential and is intended solely for the use of authorized personnel at Cedar Ridge Regional Water Authority. Distribution to unauthorized parties is prohibited.

Sentinel OT recommends engaging a qualified OT security integrator to perform a comprehensive on-site assessment and implement the remediation actions described in this report.

Sample document. Cedar Ridge Regional Water Authority is a fictional operator used to illustrate the format and depth of a Sentinel OT vulnerability intelligence report. No real utility, facility, or IP address is depicted. Addresses 198.51.100.10 and 198.51.100.11 are drawn from the IETF RFC 5737 documentation range reserved for examples.

Report ID: `pbcwud_cedar-ridge_sample_2026-04-15`