IOActive Security Advisory

Title	OleumTech Wireless Sensor Network Vulnerabilities
Discovered by	Lucas Apa and Carlos Penagos
Disclosure	Coordinated with ICS-CERT
Severity	Critical
Remediation Level	Unavailable

Affected Products

OleumTech™ Wireless Sensor Network devices

Wireless Gateways

Wireless gateways collect data from end nodes and are equipped with RS232/RS485 serial ports to communicate with backbone SCADA systems, such as RTU, EFM or PLC, and HMI, through Modbus. Multiple gateways can be added to the same network for peer-to-peer communication and sharing data. The base unit provides onboard analog inputs, discrete inputs, discrete outputs, and I/O expansion capabilities.

For more information, see:
http://www.oleumtech.com/wireless-gateways.html

Figure 1: Wireless Gateways

Wireless Transmitters

The WT series of wireless transmitters is equipped with local displays for instantly viewing process data and using the LCD for configuration. No cables, tools, or computers are required to program the device. Wireless transmitters are used to monitor conditions, such as the liquid level, pressure, flow, temperature, and triggering set-point alarm. These devices are self-contained, battery-powered, and eliminate the need for external power. They are intrinsically safe for use in hazardous locations and provide third-party device integration capabilities.

For more information, see:

http://www.oleumtech.com/wireless-sensors-transmitters-local-display.html

http://www.oleumtech.com/wireless-transmitters.html

Figure 2: Wireless Transmitters

Wireless I/O Modules

By using wireless I/O modules, users can add additional input or output points to an OleumTech wireless network over Radio Frequency (RF). These devices can be used for wireless fail safe, valve control, wellhead, emergency shutdown systems, and other industrial process monitoring and control applications. The wireless I/O modules are designed to communicate with a wireless gateway in a network for point-to-point contact. They also have Modbus master read and write capabilities.

For more information, see:

http://www.oleumtech.com/wireless-io-expansion-modules.html

Figure 3: Wireless I/O Modules

BreeZ® Software

OleumTech Wireless Sensor Network devices are managed by the BreeZ® software, which allows users to:

- Create a network
- Add devices to a network
- Define parameters
- Set transmission levels for each device

It also allows users to create a Modbus mapping table so that the collected data can be polled by a Modbus master device, such as an EFM, PLC, HMI, DCS, or RTU that is connected to a wireless gateway.

Background

OleumTech has manufactured industrial wireless solutions for almost 15 years, providing visibility to disparate assets for major Oil & Gas producers for near real-time optimization decisions, resource deployment, and regulatory compliance. OleumTech also manufacturers industrial automation systems that represents the new paradigm of remote monitoring and control for industries, such as Oil & Gas, Refining, Petro-chemical, Utilities, and Water/Wastewater.

Leading companies from a variety of industries trust the OleumTech Wireless Sensor Network. According to OleumTech, more than 160,000 OleumTech devices are deployed in the field in more than 8,000 individual wireless networks across several industry sectors, including Oil & Gas, Water/Wastewater, and Utilities. Widely known industrial companies using these devices are featured on OleumTech's website, including:

- Klinger Engineering
- Black Elk Energy
- Encana
- Kinder Morgan
- Transpower
- Anadarko

Impact

IOActive reported the vulnerabilities discussed in this section to the ICS-CERT following our vulnerability disclosure policy. Attacks can be performed remotely and executed within 40 miles with a clear line of sight to the sensor network, according to the vendor radio specifications (900mhz devices).

Figure 4: Vendor Radio Specifications

Weak Site Security Key **[CVE-2014-2362] - CVSS - 7.2 - (AV:L/AC:L/Au:N/C:C/I:C/A:C)**

According to OleumTech documentation, the "Site Security Key" reduces the likelihood that transmitted information can be accessed by unauthorized devices or cross talk between other devices operating in the area. The Site Security Key is generated using the `time64()` function from the Standard C Library. This function is a 4-byte number that corresponds to the project creation calendar time. The use of this value as a key is insecure, because an unauthenticated attacker can attempt a low number of possible combinations to guess it.

```
push    0                               ; Time
call    __time64                        ; Determine the current calendar time
add     eax, esi
add     esp, 4
mov     [esp+18h+var_4], edx
mov     edx, [edi]
push    eax
mov     eax, [edx+10h]
mov     ecx, edi
call    eax                             ; eax = &update_key
mov     eax, [esp+18h+security_enabled]
```

Figure 5: `time64()` Function

The project file of a created network is directly updated with the return value of the well-known `time64()` function. This function returns the value of time in seconds from January 1, 1970. Because this function is imported from the Windows library `Kernel132.dll` and calls the `GetSystemTimeAsFileTime` function, every project uses the system time as the Site Security Key.

Using a limited number of potential keys, an attacker can deploy a known plaintext attack Over The Air (OTA) to identify the key if RF packet protection is used for encryption. The attacker can then use this key to communicate with devices and launch other attacks over the identified nodes.

All Data Messages are Sent in Plaintext **[CVE-2014-2359] - CVSS - 8.5 - (AV:N/AC:L/Au:N/C:C/I:P/A:N)**

The OleumTech documentation states:

"*The Enhanced Site Security feature designed to provide an additional level of protection for RF packets sent and received between OleumTech devices."*

None of the devices using the 802.15.4 protocol for message transmission use the Site Security Key to encrypt OleumTech protocol data, even though the documentation states that the key is used to protect RF data. This allows attackers to identify sensor node information OTA, as well as the topology of gateways and transmitters.

Attackers can impersonate devices within the sensor network and forge packets with false temperature or pressure values using a $40 transceiver. When the gateway nodes receive this value, they transmit it to other critical machinery. Using this information, attackers can change the physical state of the current system, resulting in unknown and harmful consequences.

IOActive reproduced this attack in a practical and controlled environment involving a human-machine interface. Our demonstration showed that it is possible to attack the sensor network by injecting a fake temperature into a chemical tank. Because the temperature sensors actively control the liquid's temperature, a modification of their readings caused us to have to stabilize the system. This demonstration was first presented at Black Hat USA 2013.

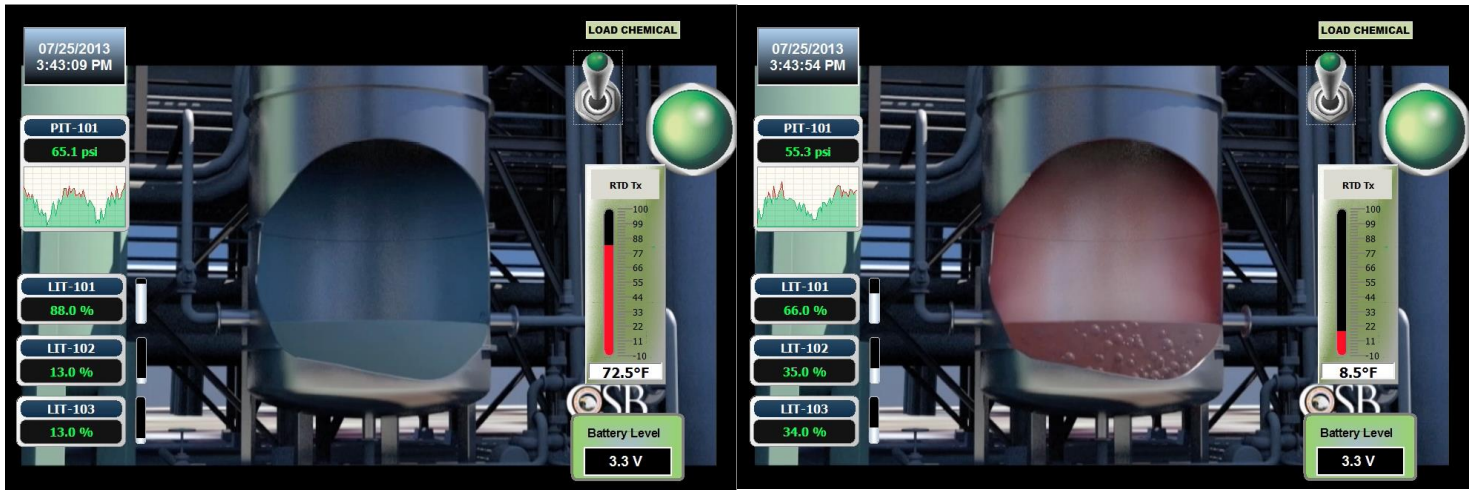

Figure 6: False Temperature Values Injected into Gateway Node

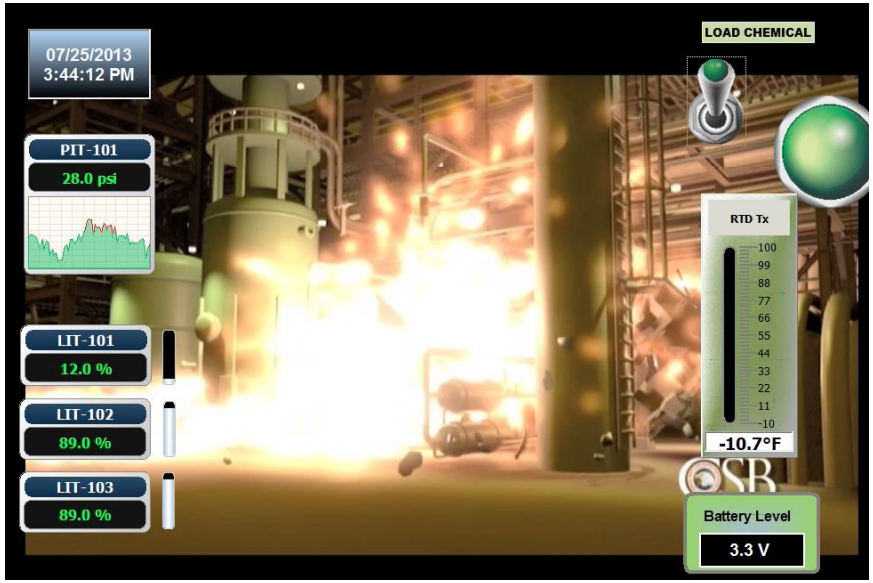

Figure 7: Chemical Cannot Tolerate Temperature and Explodes

Weak Resilience and Node Capture **[CVE-2014-2361] - CVSS - 7.2 - (AV:L/AC:L/Au:N/C:C/I:C/A:C)**

IOActive connected devices to the BreeZ software and could read the device's Site Security Key without authentication. As a result, someone who steals a device can obtain the Site Security Key and freely communicate with other devices without performing a hardware memory extraction.

Facility Denial of Service **[CVE-2014-2360] - CVSS - 5.0 - (AV:N/AC:L/Au:N/C:N/I:N/A:C)**

Attackers can send a specially crafted packet to the DH2 Gateway OTA to completely shut down the radio microcontroller until the device reboots itself a few minutes later. This attack can be persistent enough to disable any sensor reading reception for an undetermined amount of time. Attackers can launch this attack using multiple RF transmitters to disable all gateway nodes in an entire plant.

For more information, see this white paper:

http://www.ioactive.com/pdfs/Compromising_Industrial_Facilities_From_40_Miles-Away-Lucas_Apa_and_Carlos_Penagos.pdf

Solution

IOActive reported this vulnerability to CERT/CC on June 17, 2013, and CERT/CC later contacted OleumTech about the issue. OleumTech has not published a remediation or press release for this vulnerability as of the time of this advisory.

