Schneider Electric Security Notification

Security Notification – TelevisGo

13 August 2019

Overview

Schneider Electric is aware of multiple vulnerabilities in the third party UltraVNC software component embedded within the TelevisGo product.

Affected Product(s)

TelevisGo versions manufactured prior to 15th July 2019.

Vulnerability Details

CVE ID: **CVE-2019-8258**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A Buffer errors CWE-119 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2018-15361**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A Buffer errors CWE-119 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8259**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A Resource Management Errors CWE-339 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause to leak stack memory and bypass ASLR when UltraVNC software vulnerability is exploited.

Schneider Electric Security Notification

CVE ID: **CVE-2019-8260**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An Out-of-bounds Read CWE-125 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause unauthorized disclosure of information when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8261**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An Out-of-bounds Read CWE-125 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause unauthorized disclosure of information when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8262**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A Buffer errors CWE-119 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8280**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Out-of-bounds Read CWE-125 and Out-of-bounds Write CWE-787 vulnerabilities exist in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8263**

CVSS v3.0 Base Score 6.5 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

A Buffer errors CWE-119 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause denial of service (DoS) when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8264**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Out-of-bounds Read CWE-125 and Out-of-bounds Write CWE-787 vulnerabilities exist in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8265**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Out-of-bounds Read CWE-125 and Out-of-bounds Write CWE-787 vulnerabilities exist in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8266**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Out-of-bounds Read CWE-125 and Out-of-bounds Write CWE-787 vulnerabilities exist in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8267**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

An Out-of-bounds Read CWE-125 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause denial of service (DoS) when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8268**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An Incorrect calculation CWE-682 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8269**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A Buffer errors CWE-119 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause denial of service (DoS) when UltraVNC software vulnerability is exploited.

Schneider Electric Security Notification

CVE ID: **CVE-2019-8270**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

An Out-of-bounds Read CWE-125 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause denial of service (DoS) when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8271**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A Buffer errors CWE-119 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8272**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An Incorrect calculation CWE-682 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8273**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A Buffer errors CWE-119 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8274**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A Buffer errors CWE-119 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause remote code execution when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8275**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An improper access control CWE-284 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause out-of-bound data being accessed by remote users when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8276**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A Buffer errors CWE-119 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause Denial of Service (DoS) when UltraVNC software vulnerability is exploited.

CVE ID: **CVE-2019-8277**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A resource management errors CWE-399 vulnerability exists in UltraVNC embedded in TelevisGO product which could cause to leak stack memory and bypass ASLR when UltraVNC software vulnerability is exploited.

Remediation

This vulnerability is fixed in TelevisGo versions manufactured after 15th July 2019.

For units previously purchased or installed, *TelevisGo_HotFix_20190715.exe* and is available for download and install below:

https://www.eliwell.com/download/downloader.php?cat=sw&id=233

Product Information

TelevisGO is a family of devices to monitor, control and manage remote plants.

The product is based on a PC Embedded standard platform to offer greater calculation power, data filing space and easy system expansion.

Product Category - All Categories

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

TelevisGO version manufactured prior to 15th July 2019, and using UltraVNC version 1.0.9.6.1 and prior.

Schneider Electric Security Notification

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Acknowledgements

Schneider Electric recognizes Kaspersky Labs for their efforts.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *13 August 2019*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2019.08.12 11:39:36 -04'00'