Security Bulletin

SecB0001: enteliBUS 3.40 Controllers Remote Code Execution Vulnerability

Summary

First published: July 18, 2019

Description	enteliBUS controllers running firmware 3.40 R5 build 571848 or earlier versions contain a buffer overflow vulnerability which allows for remote code execution.
Affected Products	enteliBUS Manager (eBMGR), enteliBUS Manager Touch (eBMGR-TCH), enteliBUS Controller (eBCON) running firmware 3.40 R5 or earlier versions.
Recommended Action	Upgrade enteliBUS firmware to 3.40 R6 build 612850.
CVSS v3.0 Base Score	9.8 Critical
Defect Number	EBUS-2442
CVE ID	2019-9569

Description

The enteliBUS controllers running enteliBUS firmware 3.40 R5 build 571848 or earlier versions contain a buffer overflow vulnerability which allows for remote code execution.

Second generation enteliBUS controllers (eBMGR-2, eBMGR-TCH-2, eBCON-2) are not affected. These controllers can only run enteliBUS firmware 3.40 R6 and later versions which do not contain the vulnerability.

Security Bulletin

Recommended Action

Upgrade your enteliBUS 3.40 firmware to version 3.40 R6 build 612850 to remove this vulnerability.

Mitigation

It is important that buildings are updated to the 3.40 R6 version release to mitigate risk.

In addition to upgrading your enteliBUS system, Delta Controls recommends the following actions to secure your building sites:

- Do not leave building controllers exposed to the Internet.
  - If remote connections to the network are required, use a Virtual Private Network (VPN).
  - Secure your network using Tempered Networks products (available through Delta Controls).
- Regularly review and validate the list of users who are authorized to access sites and controllers.
- Ensure personnel with access to the system are knowledgeable about and are trained to use Delta Controls products and networks.
- Follow the security industries recommended practices for securing your sites. https://ics-cert.us-cert.gov/Recommended-Practices

Download

enteliBUS firmware 3.40 R6 build 612850 can be downloaded on the Version 3.40 Downloads page.

For more details about how to upgrade the firmware using Flash Loader or a USB drive, see the Solution section in KbA2313.

Link to Release Notes for enteliBUS firmware 3.40 R6

Security Bulletin

More Information

The following links provide tips and strategies to secure your Delta Controls products and building networks:

- Cybersecurity How-to Webinar for enteliWEB, DSC, eBMGR, eBCON, Network, ORCAweb
- KbA2252: Tips to Secure Delta Products

Delta Controls together with Tempered Networks offer a simple solution for securing building control networks using Host Identity Protocol (HIP).

- Tempered Networks Product Page

Acknowledgement

We would like to thank the McAfee Advanced Threat Research team for their assistance in discovering and verifying the resolution of this vulnerability.

Appendix: About CVSS

This CVSS version 3.0 vector was used to generate the score noted in this bulletin: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

All CVSS scores can be mapped to the qualitative ratings defined by the Qualitative Severity Rating Scale table (see below):

Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Security Bulletin

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments. The Base group is composed of two sets of metrics: the Exploitability metrics and the Impact metrics.

- The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component. On the other hand, the Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component.
- The CVSS v3.0 vector string is a text representation of a set of CVSS metrics. It is commonly used to record or transfer CVSS metric information in a concise form.

For more information, visit the CVSS website at: http://www.first.org/cvss/.