Security Bulletin

SecB0003: enteliWEB File Path Traversal Vulnerabilities

Summary

First published: January 21, 2020

Description	enteliWEB version 4.13 and earlier versions contain a file path traversal vulnerability which allows files on the server to be accessed by authenticated enteliWEB users.
Affected Products	enteliWEB 4.13 and earlier versions.
Recommended Action	Upgrade to enteliWEB 4.14 or newer, or apply patches to existing installations.
CVSS v3.1 Overall Score	8.2 High
Defect Number	EWEB-33141

Description

enteliWEB version 4.13 or earlier versions contain a file path traversal vulnerability which allows files on the server to be accessed by authenticated enteliWEB users. Anonymous users not logged into enteliWEB cannot exploit this vulnerability.

Recommended Action

Upgrade enteliWEB to version 4.14 or apply a security patch to existing installations, to remove this vulnerability.

17850 56 Ave Surrey BC Canada V3C 1C7 | Tel: 604.574.9444 | deltacontrols.com

Delta CONTROLS
A Delta Group Company

Security Bulletin

Mitigation

It is important that enteliWEB is updated to version 4.14, or the security patch is applied to the enteliWEB server, to mitigate risk. If the enteliWEB server is not available on the internet, the risk is significantly reduced, as an attacker would need physical access to the network to exploit the vulnerability.

In addition to upgrading or patching enteliWEB, Delta Controls recommends the following actions to secure enteliWEB:

- Implement and enforce password policies in your enteliWEB server.
- When remote access to enteliWEB is required, protect it behind a VPN or Tempered Networks system, to avoid exposing it on the internet.
- Ensure personnel with access to the system are knowledgeable about and are trained to use Delta Controls products and networks.
- Follow the recommendations described in the enteliWEB Network Hardening Guide.
- Follow the security industries recommended practices for securing your sites. https://ics-cert.us-cert.gov/Recommended-Practices

Downloads

- enteliWEB 4.14 can be downloaded here: enteliWEB 4.14 Downloads
- Patches for versions 4.13 and 4.12 can be downloaded here: enteliWEB Patches
- Patches for versions prior to 4.12 are provided upon request.

More Information

For more information on securing Delta Controls products and building networks please visit:

- Delta Controls Cybersecurity Center

Delta Controls together with Tempered Networks offer a simple solution for securing building control networks using Host Identity Protocol (HIP). For more information please visit:

- Tempered Networks Product Page

17850 56 Ave Surrey BC Canada V3C 1C7 | Tel: 604.574.9444 | deltacontrols.com

Delta CONTROLS
A Delta Group Company

Security Bulletin

Appendix: About CVSS

This CVSS version 3.0 vector was used to generate the score noted in this bulletin:

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:H/E:F/RL:O/RC:C/CR:L/IR:H/AR:H/MAV:L/MAC:L/MPR:L/MUI:N/MS:C/MC:L/MI:H/MA:H

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

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/.