Unauthenticated remote code execution vulnerability in Industrial HiVision

Date: August 18, 2017
Version: 1.0

Executive Summary

A vulnerability in the Industrial HiVision service could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system with administrator privileges. All Industrial HiVision versions are affected.

Details

The Industrial HiVision master service exposes various interface methods through a remote service, which is utilized by the Industrial HiVision client application. An attacker can bypass authentication and invoke methods that may be used to execute arbitrary commands on the server with administrative privileges.

The CVSSv3 Score is 9.8 (Critical) [1].

Impact

The vulnerability is critical to systems running the Industrial HiVision service. A successful attack has high impact on confidentiality, integrity and availability of the target system.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Network Management	Industrial HiVision	06.0.06 and lower, 07.0.02 and lower

Solution

Updates are available which fix the vulnerability.

Brand	Product Line / Platform	Product	Version
Hirschmann	Network Management	Industrial HiVision	06.0.07 07.0.03

For Help or Feedback

To view all Belden Security Advisories and Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.eu.com.

Related Links

- [1] CVSSv3 Score: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Disclaimer

THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE BULLETIN, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE BULLETIN, IS AT YOUR OWN RISK. INFORMATION IN THIS BULLETIN AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE BULLETINS AT ANY TIME.

Revisions

V1.0 (August 18, 2017): Bulletin created.