

Overall rating: High



This is a technical bulletin intended for technical audiences.

## Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Delta Electronics DOPSoft stack-based buffer overflow vulnerability. The vulnerability affects all DOPSoft versions.

## Technical Details

The affected product is vulnerable to a stack-based buffer overflow, which may allow for arbitrary code execution if an attacker can lead a legitimate user to execute a specially crafted file. A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function). This is going to have an impact on confidentiality, integrity, and availability.

Delta Electronics has declared DOPSoft as end-of-life and recommends users to use DIAScreen instead. This vulnerability does not exist on the newest version of DIAScreen.

### Exploitability Metrics

Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: Required

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

## Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify [VRM](#) with any questions or concerns you may have.

## References

- [CVE-2023-5944](#)
- [Delta Electronics DOPSoft](#)
- [VRM Vulnerability Reports](#)