December 19, 2023

Overall rating: Critical

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that CISA published ICS advisories to address vulnerabilities in the following products:

- BCU 500 – version 4.07
- UC 500E – version 10.1.0

Technical Details

Limited resources include memory, file system storage, database connection pool entries, and CPU. If an attacker can trigger the allocation of these limited resources, but the number or size of the resources is not controlled, then the attacker could cause a denial of service that consumes all available resources. This would prevent valid users from accessing the product, and it could potentially have an impact on the surrounding environment. For example, a memory exhaustion attack against an application could slow down the application as well as its host operating system.

There are at least three distinct scenarios which can commonly lead to resource exhaustion:

- Lack of throttling for the number of allocated resources
- Losing all references to a resource before reaching the shutdown stage
- Not closing/returning a resource after processing

Resource exhaustion problems are often result due to an incorrect implementation of the following situations:

- Error conditions and other exceptional circumstances.
- Confusion over which part of the program is responsible for releasing the resource.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-50707, CVE-2023-6689

- ICS Advisory – ICSA-23-353-02
- ICS Advisory – ICSA-23-353-03