Avocent® ACS 800 & ACS 8000 Security Update for CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Security Bulletin:
Processor Speculative Execution Vulnerabilities in ACS 800/8000 products

Summary

The Vertiv team is actively engaged with security research community to monitor for specific threats, partner with vendors for potential solutions, and mitigate the potential impact of security vulnerabilities to our customers and products. Two hardware based vulnerabilities have recently been discovered that affect a large portion of modern processors, including those from Intel, AMD, and ARM-based suppliers. The root of each vulnerability is that modern processors employ speculative execution features to increase overall CPU performance. Researchers have discovered a flaw in these mechanisms that can allow unauthorized access to the CPU data cache and leak the resulting information contained within.

- ACS 800: The ACS 800 employs CPUs known to be impacted to the recently disclosed speculative execution functionality vulnerabilities.

- ACS 8000: The ACS 8000 employs CPUs known to be impacted to the recently disclosed speculative execution functionality vulnerabilities.

Please use the following links for additional technical information on the specific threats: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update

In order to exploit these vulnerabilities, an attacker must be able to execute arbitrary code on the system. The ACS800/8000 products do not allow unknown code to be executed on the system. While the underlying hardware contains these vulnerabilities, attackers are not able to exploit them.