Overall rating: Critical

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware Fortinet has published a Security Advisory to address vulnerabilities in FortiNAC – multiple versions

Technical Details

- **FortiNAC - Java untrusted object deserialization RCE** - CVE-2023-33299
  A deserialization of untrusted data vulnerability [CWE-502] in FortiNAC may allow an unauthenticated user to execute unauthorized code or commands via specifically crafted requests to the tcp/1050 service.

- **FortiNAC - Argument injection in XML interface on port TCP/5555** - CVE-2023-33300
  An improper neutralization of special elements used in a command ('command injection') vulnerability [CWE-77] in FortiNAC tcp/5555 service may allow an unauthenticated attacker to copy local files of the device to other local directories of the device via specially crafted input fields. To access the copied data, however, the attacker must have an already existing foothold on the device with sufficient privileges

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-2023-33299, CVE-2023-33300
- Fortinet PSIRT Advisory - FG-IR-23-074
- Fortinet PSIRT Advisories