Severity

High

Analysis Summary

CVE-2022-23443

Fortinet FortiSOAR could allow a remote attacker to obtain sensitive information, caused by improper access control. By sending specially-crafted HTTP GET requests, an attacker could exploit this vulnerability to obtain gateway API data, and use this information to launch further attacks against the affected system.

Impact

- Information Disclosure

Indicators Of Compromise

CVE

CVE-2022-23443

Affected Vendors

- Fortinet

Affected Products

- Fortinet FortiSOAR 7.0.2
- Fortinet FortiSOAR 6.4.4
- Fortinet FortiSOAR 6.0.0
- Fortinet FortiSOAR 5

Remediation

Refer to FortiGuard Advisory for patch, upgrade or suggested workaround information.

FortiGuard Advisory