GE Gas Power
Monitoring & Diagnostics

Security Advisory

Fortigate 80C Firewall Vulnerabilities

Publication Date: December 3, 2021
Current Version: 1.0

Summary

GE Security evaluates the risk level of these vulnerabilities to customers as: LOW

CVE-2020-12812
This vulnerability is related to SSL VPN 2FA bypass where an improper authentication may result in a user being able to log in successfully without being prompted for the second factor of authentication (FortiToken) if they changed the case of their username.
https://nvd.nist.gov/vuln/detail/CVE-2020-12812

CVE-2019-5591
This vulnerability is related to FortiGate default configuration that does not verify the LDAP server identity.
https://nvd.nist.gov/vuln/detail/CVE-2019-5591

CVE-2018-13379
This vulnerability is related to path traversal vulnerability in the FortiOS SSL VPN web portal may allow an unauthenticated attacker to download FortiOS system files through specially crafted HTTP resource requests.
https://nvd.nist.gov/vuln/detail/CVE-2018-13379

Vulnerability

M&D's affected firewall product includes:

- Fortigate 80C

Impact

The impact of these vulnerabilities is negligible as this firewall is not internet-facing. It is purpose-built to secure data flow to and from the OSM device.

Consideration

Since the Fortigate 80C has reached end of life, as a natural progression of your security lifecycle management, you may wish to consider replacing the Fortigate 80C firewall with the latest M&D firewall offering that is a direct replacement providing the same security functionality as the Fortigate 80C.

GE Power Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact GE Power PSIRT at https://www.ge.com/gas-power/products/digital-and-controls/cybersecurity.