Nexus OTArmor™ Default Admin Account

Overview

GE Gas Power is informing customers operating the Nexus OTArmor 4.01 cyber security management system of a potential vulnerability present in the DCx Hardening Group Policy Object (GPO) in Active Directory.

Severity

GE Gas Power has identified this as a high-risk vulnerability that should be remediated by affected customers.

Affected Products and Versions

Nexus OTArmor version 4.01

The Nexus OTArmor 4.01 system contains VMWare vSphere ESXi 7.0 Update 2 and security Virtual Machines with Windows Server 2019 and were delivered to customers between Febuary 2022 and August 2023

Vulnerability Details

GE Gas Power has identified that a setting in DCx Hardening Policy located in Active Directory of the Nexus OTArmor system was applied incorrectly. With the incorrect setting, the built-in Administrator account created when the system was built was not properly disabled. The existence of the Built-in Administrator account presents a risk of unauthorized access to the Nexus OTArmor domain with the default credentials, potentially enabling changes to user access privileges or security policies by unauthorized personnel.

Exploitation Status

GE Gas Power Product Security has not yet observed nor received reports of any exploit attempts against Gas Power Customers.

Remediation/Mitigation

To remediate this issue, the DCx Hardening Policy must be updated in Active Directory. For support and detailed instructions, please contact the Nexus Controls technical support team to log a case and receive step by step instructions on making the necessary changes. Once completed, the Built-in Administrator account will be disabled, this change does not require any reboots of the domain controllers.

The Nexus Controls Technical Support team can be contacted by sending an email to controlsconnect@ge.com. Please reference this bulletin and provide your contact information for our team to contact you with the necessary details.

Resources

none

Contact Information

Contact your local GE Services representative for assistance or for additional information.
For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Document History

Version	Release Date	Purpose
1.0	8/29/2023	Initial Release