OCTOBER 21, 2021

NERC Lessons Learned and Alerts

Harish Vijay Kumar
Compliance Assurance

Link: Lessons Learned (nerc.com)

ieso
Connecting Today. Powering Tomorrow.

NERC Lessons Learned

Managing Underfrequency Load Shed Obligations and Service to Critical Loads during an Energy Emergency	
Interest Groups:	BA, DP, PC, RC, TO, TOP
Problem Statement:	Due to the amount of load shed during the February 2021 cold weather event, entities found it difficult to rotate customer outages while maintaining service to critical loads and underfrequency load shed (UFLS) feeders. Simultaneously, the percent of system load connected to UFLS feeders substantially exceeded the required percentage levels which created a risk of frequency overshoot and instability in the event of UFLS activation.
Lessons Learned :	When UFLS-connected load is well above the minimum required per the UFLS program, system operators (with RC and BA permission) should have the flexibility to utilize some of the UFLS “margin” from circuits normally reserved for UFLS to manually shed load and rotate outages in extreme load shed scenarios.
	Critical loads should not all receive the same level of priority, and the characteristics of a load shed event (depth/duration/season) will impact the treatment of certain critical loads. Some critical loads are able to withstand outages of several hours without having negative impacts and should therefore only be exempted from load shed in situations where load shed is expected to be of substantial duration/depth. Additionally, it is important to recognize that criticality designations must be considered in the context of the situation.

NERC Alert

Apache Software Foundation Log4j, aka Log4Shell Vulnerability

Initial Distribution: December 14, 2021

Entity Distribution:	BA,DP, GOP, GO, PA, RC, TO, TOP, TP
Problem Statement:	A critical remote code execution vulnerability in Apache Software (Java logging library Log4j, CVE-2021-44228), was identified . Successful exploitation of this vulnerability may enable an adversary to install arbitrary malicious code leading to initial access to a targeted environment or full control over impacted system. Log4j is a commonly used, open-source, logging framework in Java developed by the Apache Foundation that is used in enterprise applications and numerous cloud services (such as Apple, Apache, Steam, Redis, ElasticSearch). It is also used in open-source repositories and various industrial applications including Supervisory Control and Data Acquisition (SCADA), Energy Management Systems (EMS) and other operational technology (OT) environments.
Recommendations:	Review the following: (1) Apache Log4j Security Vulnerabilities (2) CISA Apache Log4j Vulnerability Guidance (3)Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package and (4) preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation.
	Identify whether vulnerable applications exist in the environments that leverage the Log4j library. Additionally, monitor for malicious network connections that indicate reconnaissance scanning and possibly exploitation attempts. If you have a vulnerable version(s) of Log4j Java logging library in your corporate and/or operational technology environments, immediately commence your patch management process and apply the appropriate approved patches as soon as possible

ieso
Connecting Today. Powering Tomorrow.

NERC Alert

Preparation for Potential Russian Cyber Activity against Industry from Russia-linked Actors-Level II

Initial Distribution: February 15, 2022

Entity Distribution:	BA, DP, GO, GOP, PA, RC, TO, TOP.
Problem Statement:	NERC has issued a level II recommendation to raise North American Electricity industry's preparedness to its highest possible level of potential Russian linked cyber and disinformation activity. Ah this time, NERC is not aware of a specific or credible threat to the North American electricity industry from Russia, but this proactive recommendation encourages preparedness and awareness to threat mitigation.
Recommendations:	• Entities should be aware of potential threat from ransomware during this time. • Entities and key vendors should pay extra attention to the remote access of organizational networks, particularly operational technology (OT) and Industrial control systems (ICS). • Entities should prioritize software updates that address known exploited vulnerabilities identified by Cybersecurity and Infrastructure Agency (CISA) or the E-ISAC and adopt mitigation strategies if patching is not an option. • Entities should heighten detection activities to identify potential intrusions of critical systems and better investigate anomalous activities. • Confirm an organizations entire network is protected by antivirus/anti Malware solutions. • Entities should consider proactively activating their incident response and crisis management teams. Entities should also be prepared to separate or island OT networks from corporate IT networks, consistent with pre-established plans. • Review CISA SHIELDS UP Guidance • Report any exploitation of these vulnerabilities to the E-ISAC (operations@eisac.com)

ieso
Connecting Today. Powering Tomorrow.

Thank You

ieso.ca

1.888.448.7777

customer.relations@ieso.ca

engagement@ieso.ca

@IESO_Tweets

facebook.com/OntarioIESO

linkedin.com/company/IESO

ieso
Connecting Today. Powering Tomorrow.