NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Firewall Failure After Time Limit Exceeded

Primary Interest Groups
Balancing Authorities (BAs)
Generation Operators (GOPs)
Reliability Coordinators (RCs)
Transmission Operators (TOPs)
Transmission Owners (TOs) that operate an Energy Management System (EMS)

Problem Statement
Due to a firmware error, a firewall stopped processing network traffic without proper failover after an internal run-time limit was exceeded. This resulted in persistent remote terminal unit (RTU) communication issues.

Details
A firewall firmware security patch issued by the firewall vendor was applied to an entity's equipment, which unknown to all parties at the time, contained a process runtime limit of 213.5 days.

After reaching reaching the 213.5 day limit of uptime, the entity experienced a loss of all SCADA-EMS RTU communications. The system operator called in-house SCADA-EMS support and started notifying all neighboring TOPs and requested assistance. The entity's SCADA-EMS Manager remoted into the SCADA-EMS system and verified that SCADA-EMS system processes were functioning but found there was a network issue causing loss of communication with the field RTUs. The entity's SCADA-EMS analyst arrived on site and verified that SCADA-EMS system was functioning normally, but found that an outside interface of an online polling firewall was blocking traffic; the online polling firewall software had failed. The network administrator attempted to failover to the backup firewall. This did not resolve the issue because both firewalls were experiencing the same firmware issue due to the similar uptimes of the firewall software. Both firewalls remained online and both were trying to process traffic.

The network administrator rebooted the backup polling firewall and shut down the outside interface on the online polling firewall. After that, all communication circuits began to be restored.

After investigation and discussion with the firewall vendor, it was determined that about two months prior to the event, the vendor had identified the runtime bug and notified their users via a blog post. The post gave detailed interim advice on how to check the elapsed uptime and to reboot the firewall "proactively" prior to hitting the limit while the vendor worked on a patch. A followup Field Notice about a week before the event provided additional details. Notification of the patch and and a link to it were provided in subsequent technical bulletin.

The entity had a focus on security patching. Security bulletins from the vendor were monitored and security patches were promptly tested and applied. In this case, the interim rebooting advice and eventual patch were provided in the vendor site blog, field notices, and technical bulletins, which were not processed with the same priority as security bulletins.

Corrective Actions

The entity rebooted the backup firewall then shut down the outside interface on the online polling firewall to force a failover. This restored network traffic and RTU communications.

Following the vendor interim advice, the entity then scheduled proactive reboots of the control center firewalls and other affected firewalls.

Later, the firewall firmware was upgraded to a new release that did not have the same limitation.

The entity now uses the same level of priority for review for technical bulletins as the security bulletins.

Lesson Learned

To prevent recurrence of the issue, maintain network devices on a planned schedule in accordance with the latest vendor information, security bulletins, technical bulletins, and other recommended updates.

If available, entities should enroll in automated notification services for these updates.

NERC's goal with publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC requests that you provide input on this lesson learned by taking the short survey provided in the link below.

Click here for: Lesson Learned Comment Form

For more Information please contact:

NERC – Lessons Learned (via email)	MRO – Event Analysis
Source of Lesson Learned:	Midwest Reliability Organization
Lesson Learned #:	20180802
Date Published:	August 7, 2018
Category:	Transmission Facilities

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.