Lesson Learned

Risks Posed by Firewall Firmware Vulnerabilities

Primary Interest Groups

Transmission Operators (TOPs)
Transmission Owners (TOs)
Generation Operators (GOPs)
Generation Owners (GOs)
Distribution Providers (DPs)
Reliability Coordinators (RCs)
Balancing Authorities (BAs)

Problem Statement

A vulnerability in the web interface of a vendor's firewall was exploited, allowing an unauthenticated attacker to cause unexpected reboots of the devices. This resulted in a denial of service (DoS)[1] condition at a low-impact control center and multiple remote low-impact generation sites. These unexpected reboots resulted in brief communications outages (i.e., less than five minutes) between field devices at sites and between the sites and the control center.

Details

A registered entity with a low-impact control center experienced brief (i.e., less than five minutes) outages of internet-facing firewalls that controlled communications between the control center and multiple remote generation sites and between equipment on these sites. The affected firewalls were all perimeter devices that served as the outer security layer. These outages had no impact to generation. Seeing several of these outages at different sites raised suspicion and led to a more in-depth investigation. This investigation revealed that the communications outages were due to reboots of the firewalls at each of the sites. The entity's system monitoring tools also provided notification of the firewall reboots. These records show the firewall reboots occurred over a 10-hour time period with each firewall showing offline status for less than five minutes.

After an initial internal investigation, the entity decided that, in order to fully characterize the nature of the reboots and the potential causes, the firewall manufacturer should review logs. Subsequent analysis determined that the reboots were initiated by an external entity exploiting a known firewall vulnerability. After receiving this notification, the entity initiated their event reporting procedure as dictated by their cybersecurity incident response plan. Along with identifying the cause of the reboots, the firewall manufacturer offered a firmware update that would address the vulnerability. The entity assessed the update details and determined it was appropriate to deploy immediately. The entity first deployed the

[1] See previous NERC Lessons Learned LL20181001, "Networking Packet Broadcast Storms" for a discussion of a self-inflicted problem having similar symptoms to a DoS attack.

firmware patch on a firewall within a non-critical environment[2] at the entity's control center that would not impact operational assets and monitored the changes for any adverse effects. After seeing no adverse effects, the entity deployed the firmware patch at an operational generation site that night. After monitoring traffic in the production environment overnight and early the following morning, the entity deployed the update to all remaining BES assets that had common hardware with the firmware vulnerability.

Corrective Actions

After completing mitigation efforts to address the immediate risk posed by the firmware vulnerability, the entity performed an internal assessment to identify internal process improvements to reduce the likelihood of an event with a similar cause from happening again. Given that a firmware update to address the exploited vulnerability had been released prior to the event, the entity's process for assessing and implementing firmware updates was reviewed. Based on this review, the entity decided to implement a more formal and more frequent review of vendor firmware updates that would be tracked within internal compliance tracking software. It should be noted that the entity was already working to develop internal procedures to support this process; however, these were not completed or being practiced at the time of the event. Additionally, the entity now utilizes firewall rules that restrict allowable traffic to the minimum required to operate the assets.

Lesson Learned

Even in cases involving low-Impact BES assets, an entity should strive for good cyber security policies and procedures. Consider some of the following lessons:

- Follow good industry practices for vulnerability and patch management.
    - Close monitoring of vendor firmware releases and their implementation is a key element of a strong cybersecurity posture. Firewall firmware updates need to be reviewed as quickly as possible after release for risk and applicability.
    - Testing in a development (or "sandbox") environment prior to deployment is the best way to check for the patch's potential to introduce new problems.
- Reduce and control your attack surface.
    - Have as few internet facing devices as possible.
- Use virtual private networks.
- Use access control lists (ACLs) to filter inbound traffic prior to handling by the firewall; minimize the traffic through a denial by default configuration with whitelisting for the allowed and expected IP addresses. Limit outbound traffic similarly for information security purposes.

[2] Even in an emergency, still test before applying patches to control systems to ensure no adverse effects upon patch implementation, preferably testing in a development environment. If that is not possible, then test in a less critical part of the environment as was done in this case. Also, when designing the network, include the ability to perform maintenance on VPN terminators without having to take down the edge firewall because if it is hard or expensive to do, the chances it won't be completed increase.

- Layer defenses. It is harder to penetrate a screening router, a virtual private network terminator, and a firewall in series than just a firewall (assuming the ACLs and other configurations are appropriate).
- Segment your network. Restrict lateral communication to necessary and expected traffic to reduce the impact of a breach.
- Know your exploitable vulnerabilities so you can pursue fixes.
  - Maintain awareness of vulnerabilities and understanding of those in your environment through product vendor websites and user groups and third party resources, such as the National Vulnerability Database[3], SANS Internet Storm Center[4], Exploit Database[5], etc.
  - Consider asking the Department of Homeland Security under the "National Cybersecurity Assessment and Technical Services (NCATS) program[6]" (or a security vendor) to conduct external vulnerability scanning.
  - Join the Electricity Information Sharing and Analysis Center (E-ISAC)[7].
- Monitor your network.
  - System performance monitoring increases the likelihood that brief communications outages with little actual impact to generator operations will be more closely investigated. This is how this lesson learned came to be.
  - Use tools for firewall log analysis to detect events and support post-event investigations. This will provide information about the nature of attacks and exploits used.
  - Report attacks and suspicious activity to the E-ISAC.
- Employ redundant solutions to provide resilience and on-line maintenance capabilities:
  - Of the entity's sites impacted by the firewall reboot, not all experienced communications disruptions. Following the event, it was discovered that the sites running firewalls in high-availability/redundant pair configuration maintained communications during the reboots. At sites utilizing this design, the secondary firewall maintained communications while the primary firewall rebooted.
  - Firewall redundancy preserves functionality in the event of a single firewall failure.
  - Firewall redundancy reduces impact of firmware updates since each firewall can be updated independently without interrupting communications during the update process.

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 is asking

[3] National Vulnerability Database https://nvd.nist.gov/
[4] SANS Internet Storm Center https://isc.sans.edu/
[5] Exploit Database https://www.exploit.db.com/
[6] National Cybersecurity Assessment and Technical Services https://www.us-cert.gov/resources/ncats
[7] Electricity Information Sharing and Analysis Center https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx

entities who have taken action on this lesson learned to respond to 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)	WECC Event Analysis
Source of Lesson Learned:	Western Electric Coordinating Council
Lesson Learned #:	20190901
Date Published:	September 4, 2019
Category:	Communications

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.