NERC Lessons Learned:

“Risks Posed by Firewall Firmware Vulnerabilities”

Donnie Bielak
Reliability Engineering

Published

- **Title**
  - Risks Posed by Firewall Firmware Vulnerabilities
- **Source of Lesson Learned**
  - Western Electric Coordinating Council (WECC)
- **Date Published**
  - September 4, 2019

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 condition at a low-impact control center and multiple remote low-impact generation sites
  - No impact to generation
- These unexpected reboots resulted in brief communications outages (less than five minutes) between field devices at sites and between the sites and the control center
- Reboots were initiated by an external entity exploiting a known firewall vulnerability
  - Manufacturer offered a firmware update to address the vulnerability

Lessons Learned

- Follow good industry practices for vulnerability and patch management
- Reduce and control your attack surface
- Use virtual private networks
- Use access control lists (ACLs) to filter inbound traffic prior to handling by the firewall
- Layer defenses (i.e., screening router, VPN terminator, firewall)
- Segment your network
- Know your exploitable vulnerabilities so you can pursue fixes
- Monitor your network
- Employ redundant solutions to provide resilience and on-line maintenance capabilities

Links

https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf