Amnesia:33 - a Wakeup Call for Health Informatics

Quick summary

Amnesia: 33 is vulnerability in several open source TCP protocol stacks. Forescout Research Labs discovered 33 vulnerabilities impacting millions of IoT, OT and IT devices that present an immediate risk for organizations worldwide [1]

Note that [1] deals with open source protocol stacks for TCP: open source stacks: picoTCP, FNET, uIP, nut/NET. Four of these vulnerabilities are critical exposing "remote code execution, "denial of service" and "Data exfiltration" attacks.

Recommended remediation:

Mitigation	*Comment*
1. Asses risk and exposure	*Should be carried out in any breach, configuration change or annual review of security infrastructure*
2. Rely on internal DNS servers	*This measure is difficult to implement*
3. Disable or block IPv6 traffic	*This measure is catastrophic and would eliminate the currently most frequently used Internet routing protocol, leaving only IPv4*
4. Segment devices	*This measure isolates the device and is reasonable*
5. Patch vulnerable devices	*This measure is the best response.*
6. Monitor for malformed packets	*This measure should be an active action for all clinical IoT devices.*

Analysis

i. The threat environment has continually evolved over the last 2 years. *WannaCry* was a wakeup call; *Sunburst* is the most recent profound attack on US institutions. See Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials, National Security Agency | Cybersecurity Advisory [6]

ii. open source software has been a contributing factor to the breaches

iii. the problems eventually get fixed

iv. the threat environment is becoming increasingly hostile

v. Approaches that probably work: Zero Trust

vi. Remember the last serious open source SSL vulnerability, Heartbleed, For Heartbleed Bug, see [3].

Lessons learned from breach History (see [6])

- ..lack of a proper risk analysis as a major contributing factor in breaches to health data..
- ..entities have migrated ePHI to an unsecure server or application without conducting an evaluation to determine how the security of its ePHI would be affected..
- ..of access controls that were not implemented… and .. entities are not considering access controls at the network level..
- ..OCR's investigations continue to reveal that entities are deficient in their implementation of these required review processes..
- ..entities fail to respond effectively and promptly to security incidents..

Amnesia:33 - a Wakeup Call for Health Informatics

Changes in the threat

HHS breach history indicates that a growing number of breaches are due to patch fidelity.

Verizon Report indicates 3,950 breaches over the last year. 45% due to hacking on70% of the systems by external actors. Only 8% due to misuse which represents a change in the sources.

Recommendations

a) A frequent reminder for IT staff to maintain patch currency should be standard operating practice.
b) For clinical IoT devices all open and vendor software included in the product should be itemized
c) Make an extra effort to conduct a proper risk analysis when a breach occurs, annually and whenever the configuration changes
d) Organize, train and practice incident response at least once a year

References

[1] Amnesia:33, Forescout Research Labs discovered 33 vulnerabilities impacting millions of IoT, OT and IT devices that present an immediate risk for organizations worldwide., https://www.forescout.com/research-labs/amnesia33/

[2] Authentication Flaws Found Again in GE Medical Imaging Gear, https://www.govinfosecurity.com/authentication-flaws-found-again-in-ge-medical-imaging-gear-a-15548

[3] SSL Heartbleed vulnerability, https://heartbleed.com

[4] Security Outcome Study 2020, cisco, cisco.com/go/securityOutcomes

[5] IoT Security, Forescout, https://www.forescout.com/company/resources/internet-things-solution-brief/

[6] Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials, https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF

[7] HHS Annual Report to Congress Breaches of Unsecured Protected Health Information, for 2018, U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

[8] Data Breach investigations Report 2020, Verizon