DREAD Threat Analysis

Aug 20, 2021

TEAM B

Suresh Melvin Sigera, Kikelomo Obayemi, and Japhet I Ndhlovu

DREAD Rating

	Maximum Risk	**No Risk**
Damage Potential	An attacker can gain full access to the system; execute commands as root/administrator	Leaking trivial information
Reproducibility	The attack can be reproduced every time and does not require a timing window	The attack is very difficult to reproduce, even with knowledge of the security hole
Exploitability	No programming skills are needed; automated exploit tools exist	The attack required a skilled person and in-depth knowledge every time to exploit
Affected Users	All users, default configuration, key customers	A very small percentage of users; obscure features; affects anonymous users
Discoverability	Vulnerability can be found using automated scanning tools	The vulnerability is obscure, and it is unlikely that it would be discovered

Case Study: iStan medical mannequin

DREAD Composite Risk Categories

Risk Rating	DREAD Score	Risk Description
Critical	3	A critical finding or vulnerability should be considered immediately for review and resolution. The exploitation of critical vulnerabilities is relatively easy and can lead directly to an attacker gaining privileged access (root or administrator) to the system. Findings with this risk rating, if not quickly addressed, may pose risks that could negatively affect business operations or business continuity
Medium	2	Moderate risk finding or vulnerabilities should be considered once the high critical and severe risks have been addressed. These vulnerabilities may leak sensitive data that an attacker can use to assist in the exploitation of other vulnerabilities. Moderate findings do not pose a substantial threat to business operations
Low	1	Low-risk findings are informational and do not pose a significant risk to the environment.

Finding Summary

Threat: Potential For Brute Force Attack, Denial of Service (DoS)		
Category	**Score**	**Rationale**
Damage	3	Significant damage to access point configuration

Reproducibility	3	Well known vulnerability which can be reproduced with relative ease using widely available tools. Such as Parrot OS, BlackArch, Knoppix STD, Kali Linux
Exploitability	3	Easy to exploit as the attack was made by undergraduate students (not skilled penetration testers) who only had a few months study on network security. Open source tools were used.
Affected Users	3	All medical staff that are receiving training.
Discoverability	3	Discoverability is assumed to be at the highest rating (Howard & LeBlanc, 2003)
DREAD Score: 15		

Potential Mitigations

The medical mannequin relies on two types of dependencies: direct and indirect

Direct

- Properly configured access point and secure network configuration (e.g. WPA-2)
- Disabling Static and enabling dynamic cypher for TLS
- Use of TLS 1.2 or above, Currently, the most secure and most recommended combination of these four is: Elliptic Curve Diffie–Hellman (ECDH), Elliptic Curve Digital Signature Algorithm (ECDSA), AES 256 in Galois Counter Mode (AES256-GCM), and SHA384
- Setup an intrusion detection system (IDS) and Active Network Monitoring mitigate the risk of DoS attacks
- Prevention of Spoofing (filtering to detect inconsistencies) to ensure legitimate traffic

Indirect

- Security regulations may help enforce strict(er) security standards for the manufacturing of such medical equipment

References

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Healthcare Information Systems and Technology (Sighealth).

Howard, M. and LeBlanc, D.(2003) *Writing secure code*. Pearson Education.