Dread Rating

Threat	D	R	E	A	D	Total	Rating
Attacker obtains Authentication Credentials by Brute-Force Attack	3	2	3	3	3	14	High
DOS Attack making the application unusable	1	3	3	3	2	12	High
Eavesdropping/communication sent in clear text	2	3	3	1	3	12	High
High Risk (12-15)							
Medium Risk (8-11)							
Low Risk (5-7)							

Threat Description	Attacker obtains authentication credentials by Brute force attack
Threat target	Wireless Access Point
Risk rating	High
Attack techniques	Use of Brute force software (Reaver and BackTrack 5)
Countermeasures	Strong password policies, MFA (Multi-Factor Authentication), limitation of failed login attempts, implementation of user lockouts, continuous log monitoring

Threat Description	DOS Attack making the Istan application unusable
Threat target	iStan Muse software (Briowser based application)
Risk rating	High
Attack techniques	Using a Linux testing tool called HPING3
Countermeasures	Next-Gen Firewalls with IDS and IPS, monitoring & analysing traffic flow patters

Threat Description	Eavesdropping/communication sent in clear text
Threat target	Medical devices communicating on an unencrypted network
Risk rating	High
Attack techniques	Scanning tools, Nmap, Wireshark, etc - Entry point for majority of other attacks
Countermeasures	Encryption end-to-end

Group 1

DREAD	Improper credential management and authentication	Improper access control, privilege management, and authorization	Stack and Buffer Overflow
Damage	3	3	1
Reproducibility	2	1	3
Exploitability	1	1	2
Affected users	3	3	2
Discoverability	2	2	2
Σ	11	9	10
Ø	2.2	1.8	2

low issue = 1 **medium issue = 2** **high issue = 3**

Xu et al. (2019)

Potential mitigations:

Improper credential management and authentication	Improper access control, privilege management, and authorization	Stack and Buffer Overflow
Education of the staff (the human factor)	Education of the staff (the human factor)	Appropriate network size
Encryption	Hierarchical privilege management	Network firewalls
Two-Factor authentication	Physical protection of the end devices from access	Detection of irregular inquiries (Controller-agent)

References:

- Xu, Y., Tran, D., Tian, Y., Alemzadeh, H. (2019) Poster Abstract: Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices. *2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies. (CHASE)*, 2019, pp. 23-24, doi: 10.1109/CHASE48038.2019.00017.