Findings and Recommendations

5.1 DREAD Scoring Criteria

Damage Criteria	Critical (Score: 10)	High (Score: 7)	Medium (Score: 4)	Low (Score: 1)
Damage Potential	An attacker can gain full access to the system; execute commands as root/administrator	An attacker can gain non-privileged user access; leaking extremely sensitive information	Sensitive information leak; Denial of Service	Leaking trivial information
Reproducibility	The attack can be reproduced every time and does not require a timing window	The attack can be reproduced most of the time	The attack can be reproduced, but only with 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	A novice hacker/programmer could execute the attack in a short time	A skilled programmer could create the attack, and a novice could repeat the steps	The attack required a skilled person and in-depth knowledge every time to exploit
Affected Users	All users, default configuration, key customers	Most users; common configuration	Some users; nonstandard configuration	Very small percentage of users; obscure features; affects anonymous users
Discoverability	Vulnerability can be found using automated scanning tools	Published information explains the attack. The vulnerability is found in the most commonly used feature	The vulnerability s in a seldom used part of the product, and few users would come across it	The vulnerability is obscure and it is unlikely that it would be discovered

5.2 DREAD Composite Risk Categories (Key)

Risk Rating	DREAD Score	Risk Description
Critical	40-50	A critical finding or vulnerability should be considered immediately for review and resolution. 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 impact business operations or business continuity.

High	25-39	A severe finding or vulnerability should be considered for review and resolution within a short time frame. These vulnerabilities can lead to an attacker gaining non-privileged access (standard user) to a system, or the vulnerability can be leveraged to gain elevated level of access.
Medium	11-24	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	1-10	Low risk findings are informational and do not pose significant risk to the environment.

5.3 Remediation Effort Required (Key)

Effort Rating	Effort Description
High	Significant multi-resource effort that may span over a considerable amount of time. May require a network architecture change or the purchase of additional security products.
Medium	One to several days requiring moderate amounts of resources.
Low	Less than a day requiring only a minimal amount of resources.

5.4 Finding Summary

This section summarizes the findings documented in this report. The findings are ordered based on a weighted score of the severity.

Finding	DREAD	Remediation	Result
Critical Risk Findings (40 – 50)			
x			
High Risk Findings (25 – 39)			
Medium Risk Findings (10 – 24)			
Low Risk Findings (1 – 9)			

5.5 Summary of findings by category of risk.

- **High Risk / Low Effort**: High priority, quick fixes that can be address with little time and effort.
- **High Risk / High Effort**: Mitigation of discovered vulnerability requires financial investment, and continued effort over time. Remediation will not be instant, and the business must decide what order to mitigate.

- **Low Risk / Low Effort**: Fixes that should be addressed after High / Low are fixed, and after High / High are road mapped.
- **Low Risk / High Effort**: Low priority issues that should be taken care of when time and resources allow.

High Risk / Low Effort	High Risk / High Effort
Low Risk / Low Effort	Low Risk / High Effort