External Penetration Test Report

PEN-DOC-202308190007

Golden Egg Labs, INC., https://goldenegglabs.com

19-08-2023

Contents

1 Project Overview **3**
1.1 Description 3

2 Executive Summary **4**
2.1 Summary of Findings Identified 5
2.2 Scope 6
2.2.1 In Scope 6
2.2.2 Out of Scope 6
2.3 Methodology 7
2.4 Recommendations 8

3 Findings and Risk Analysis **9**

4 Additional Notes **10**

1 Project Overview

1.1 Description

Family Life Communications consists of Family Life Radio and Intentional Living. About Family Life Radio is a network of Christian radio stations reaching more than 15 million people in our broadcast area, with 42 radio stations across the United States.

2 Executive Summary

Golden Egg Labs, INC. (GEL) was contracted by Family Life Communications, INC. (FLC) to conduct an external penetration test in order to examine the susceptibility to exploitation from a remote attacker attempting to gain acces to the internal network without host resources or inside knowledge. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against FLC with the goals of:

- Enumerating all possible entry points accros the attack surface and locating potential vulnerabilities.

- Identifying if a remote attacker could penetrate FLC's defenses through exploitation.
- Determining the impact of a security breach on the internal infrastructure and availability of FLC's information systems.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-1151 with all tests and actions being conducted under controlled conditions. Initial reconnaissance of the MegaCorp One network resulted in the discovery of a misconfigured DNS server that allowed a DNS zone transfer. The results provided us with a listing of specific hosts to target for this assessment. An examination of these hosts revealed a password-protected administrative webserver interface. After creating a custom wordlist using terms identified on the MegaCorp One 's website we were able to gain access to this interface by uncovering the password via brute-force. An examination of the administrative interface revealed that it was vulnerable to a remote code injection vulnerability, which was used to obtain interactive access to the underlying operating system. This initial compromise was escalated to administrative access due to a lack of appropriate system updates on the webserver. After a closer examination, we discovered that the compromised webserver utilizes a Java applet for administrative users. We added a malicious payload to this applet, which gave us interactive access to workstations used by MegaCorp One's administrators. Using the compromised webserver as a pivot point along with passwords recovered from it, we were able to target previously inaccessible internal resources. This resulted in Local Administrator access to numerous internal Windows hosts, complete compromise of a Citrix server, and full administrative control of the Windows Active Directory infrastructure. Existing network traffic controls were bypassed through encapsulation of malicious traffic into allowed protocols.

2.1 Summary of Findings Identified

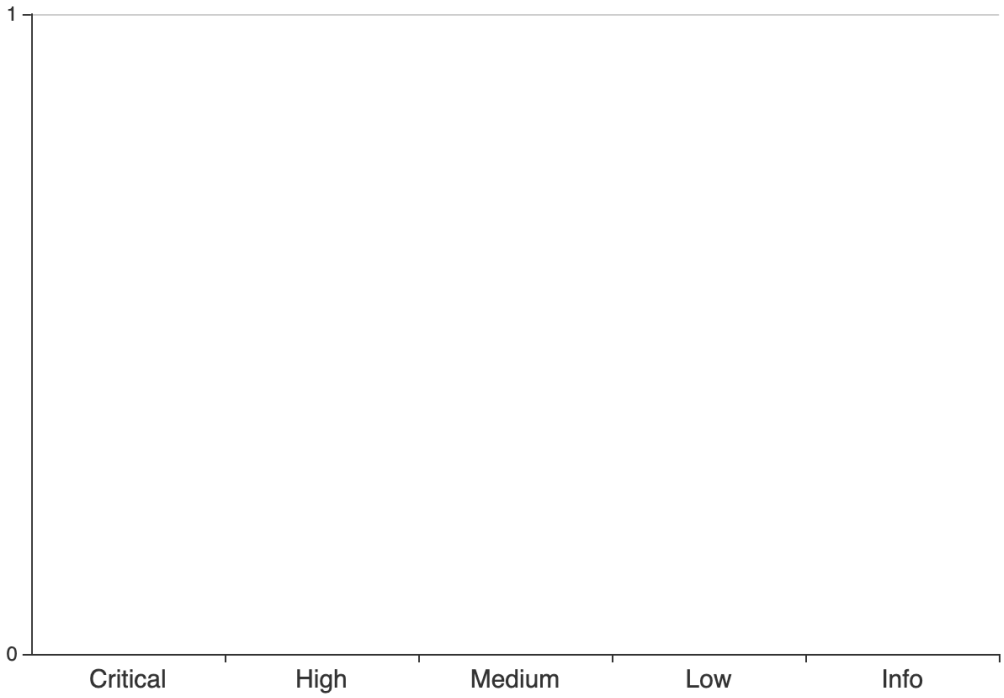

Figure 1: Executive Summary

Figure 2: Breakdown by Categories

2.2 Scope

2.2.1 In Scope

TBC

2.2.2 Out of Scope

TBC

2.3 Methodology

TBC

2.4 Recommendations

TBC

3 Findings and Risk Analysis

4 Additional Notes