### Penetration Test Executive Summary

Peter Zegarek, Caden Effrece, Evan Quinn, Charlize Aponte, Bharath Reddy, Tapiwanashe Mutumhe, Henry Cort

Stamford Health

### **Executive Summary**

During our penetration testing for Stamford Health, several security vulnerabilities and risks were identified across their web infrastructure and publicly available data sources. This test was conducted from a purely open-source standpoint, and no vulnerabilities were exploited, following the scoping document. The most critical finding involved an exposed API key on a publicly facing page of the Stamford Health website. This key could be very easily exploited by malicious actors to access other data endpoints without authorization. This same API key was found to be unchanged over the span of about a week, raising concerns about the lack of API key rotation. This API key could grant ongoing access tot hackers, potentially exposing the organization, and is a live vulnerability that could be exploited at any moment. Another critical vulnerability is the existence of plain usernames and passwords located in network packets sent when users attempt to access the Stamford Hospital website. This vulnerability can allow potential attackers to gain personal information of Stamford Hospital patients and access their private data.

Further investigation revealed several instances of employee and organizational data that could be exploited. This included sensitive personal information, such as employee ID badge pictures, names, and even footage showing an employee’s ID number and clocking out. This video also notified the Pen Testers of the fact that Stamford Health ID numbers are only 4 digits long, leaving the organization very exposed to ID badge guessing, employee fraud and impersonation. Additionally, the breach of the third-party service provider Blackbaud, which affected fundraising data between February 7 and May 20, 2020, raised concerns about the compromise of further confidential data. We also identified unsecured certificate expiration dates, which could leave the organization vulnerable to man-in-the-middle attacks or other security threats. Also discovered was the COO’s email address, and the signatures of multiple high-level employees at the organization.

### **Risk Assessment & Recommendations**

The exposed API key and the seeming lack of key rotation shows a potential high-level security risk, as malicious actors could abuse this access for unauthorized operations or data extraction. To mitigate this risk, we recommend immediate change of the exposed API key, followed by a review of all API keys and adding rotation policies. Additionally, we strongly suggest API keys are hidden from public view wherever possible, to mitigate the risk of any leaks.

Having cleartext usernames and passwords in network packets is a serious security risk because it exposes sensitive information to attackers. If these packets are intercepted, attackers can easily steal login credentials. This is especially dangerous in environments like healthcare, where attackers could steal patient data, leading to privacy violations and legal issues. The risk becomes even worse if the attacker intercepts the login details of an administrator or someone with higher privileges. In that case, they could gain full control over systems, compromising more sensitive data or even shutting down critical services. To protect against this, it's crucial to use secure methods like encryption or hashing to ensure that passwords and other sensitive information remain private and safe during transmission.

The exposure of employee and organizational information through publicly accessible content is another critical vulnerability. The organization should review its public-facing websites and systems to ensure that no personal or sensitive employee data is exposed. This includes social media presence. Data access policies should be revisited to ensure compliance with data protection standards, and systems should be implemented to ensure that sensitive data is not inadvertently exposed through visual or digital means. Employees should be trained on physical cybersecurity practices and should understand the importance of keeping an employee ID badge/number secure.

The discovery of the Blackbaud breach highlights the importance of reviewing third-party vendors and their security practices. We recommend a thorough audit of all third-party partnerships and access points, along with strengthening contracts to enforce stricter security measures. There should also be specific incident response plans in place in case the third-party partners do get breached in any way.

Finally, ensuring the security of certificates by implementing timely renewals and proper management practices will reduce the chances of system compromise due to expired certificates.

**Risk Report**:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Findings** | **Risk Level** | **Mitigation Recommendations** |
| **Domain & DNS Risks** | - Domain registered via GoDaddy (privacy-enabled).  - MX records managed by Mimecast (ASN 30031). | Medium | - Monitor DNS configurations for unauthorized changes.  - Enforce DNSSEC to prevent spoofing. |
| **Subdomain Exposure** | - **38 subdomains** found, including testing environments (e.g., qa, uat).  - Most used IP: 20.119.0.59 (9 subdomains). | High | - Remove/secure unused subdomains.  - Restrict access to internal/testing environments. |
| **Email Security** | - Predictable email format: [{f}{last}@stamfordhealth.org](mailto:%7bf%7d%7blast%7d@stamfordhealth.org).  - Accept-all SMTP server detected. | High | - Implement DMARC/DKIM/SPF to prevent spoofing.  - Disable "accept-all" email servers. |
| **Third-Party Dependencies** | - Reliance on GoDaddy (DNS), Mimecast (email), and Oracle (hosting). | Medium | - Audit third-party SLAs and incident response protocols.  - Diversify critical services. |
| **Data Exposure** | - Public LinkedIn profiles expose employee roles (e.g., "Director of Nursing").  - Employees post photos with badges or videos including badge ID | Low-Medium | - Train staff on social engineering risks.  - Limit sensitive details in public profiles. |
| **Network Infrastructure** | - Oracle BMC (ASN 31898) hosts mail01.health.stamfordhealth.org. | Medium | - Segment internal networks.  - Monitor for unusual traffic to/from critical servers. |
| **API Key Exposure** | - API Key is publicly viewable in network packet from website. | High | - Change Exposed API key  - Implement API key rotation practices |
| **Cleartext Passwords** | -Unhashed usernames and passwords were found in network packets sent to and from Stamford Hospital website portal | High | -Change packet configuration to hashed usernames and passwords |
| Certificate & API Exposure | SSL misconfigurations on mychart.stamfordhealth.org; exposed API key in Yext integration | High | - Add DNS CAA, enable OCSP, remove root anchor  - Rotate API keys, enforce CSP & SRI policies |

### **API Key Tracking System:**

|  |  |  |  |
| --- | --- | --- | --- |
| **API Reference** | **Category** | **Last Scanned** | **Next Audit Due** |
| DNS-001 | Domain & DNS Risks | 2025-05-04 | 2025-08-04 |
| SUB-001 | Subdomain Exposure | 2025-05-03 | 2025-06-03 |
| EMAIL-001 | Email Security | 2025-05-05 | 2025-07-05 |
| THIRDPARTY-001 | Third-Party Dependencies | 2025-04-28 | 2025-10-28 |
| DATA-001 | Data Exposure | 2025-05-01 | 2026-05-01 |
| NETWORK-001 | Network Infrastructure | 2025-04-30 | 2025-09-30 |
| API-002 | Yext JS Integration | 2025-04-30 | 2025-07-30 |

**Risk Prioritization:**

|  |  |  |
| --- | --- | --- |
| **Risk Level** | **Count** | **Examples** |
| **High** | 4 | Predictable email formats, exposed subdomains, exposed api keys, cleartext passwords in network packets |
| **Medium** | 3 | Third-party dependencies, DNS misconfigurations, network segmentation, public employee data (badge number). |
| **Low** | 1 | Public employee data (LinkedIn). |

### **Action Plan**

1. **Immediate (0–30 days):**
   1. Disable "accept-all" email servers.
   2. Remove unused subdomains (e.g., qa, uat).
   3. Change exposed API key and implement key rotation policies.
   4. Limit client-side exposure of third-party API keys (e.g., through proxying or obfuscation).
   5. Remove cleartext passwords in packets
2. **Short-Term (30–90 days):**
   1. Implement DMARC/DKIM/SPF for email security.
   2. Conduct employee phishing training.
3. **Long-Term (90+ days):**
   1. Migrate critical services to redundant providers.
   2. Regular penetration testing and subdomain audits.
   3. Introduce more complex employee badge numbering.
   4. Establish vendor risk management reviews for all third-party APIs and services.

### **Conclusion**

In conclusion, Stamford Health’s network, systems, and processes have been found to have significant security vulnerabilities. Immediate action is required to address these issues, including securing exposed API keys, improving internal employee verification protection, reviewing third-party vendor security, and ensuring proper certificate management. The identified weaknesses pose substantial risks to both internal data and the physical security of the organization, potentially leading to severe consequences if left unresolved.