statusgator

Monitoring the world's
cloud services since 2015

Nimble Industries, Inc.
1244 S. Evergreen Dr.
Phoenixville, PA 19460
hi@statusgator.com

StatusGator Security Checklist

StatusGator operates at all times with the security of our application and our customer's data in mind.

We follow MVSP, the Minimum Viable Secure Product security checklist[1], on which this checklist is based.

Last updated: October 27th, 2023

[1] Minimum Viable Secure Product: https://mvsp.dev/

Table of Contents

You can read about all the security controls required of this checklist, by reading the control list[2] and FAQs[3]. The checklist is based on the Dropbox' Vendor Security Model Contract (VSMC)[4], and Google's Vendor Security Assessment Questionnaire (VSAQ)[5].

1. Business controls

1.1 Vulnerability reports

StatusGator publishes a comprehensive Vulnerability Disclosure Policy[6] on its website.

We provider a single point of contact for all reports: security@statusgator.com

All reports are reviewed and triaged within 24 hours. Although actionable reports are rare, we do pay out bounties when appropriate and respond to all reports as needed.

1.2 Customer testing

Customers on our Enterprise plan are granted access to a deployed app environment that replicates production but without production data. This is used for penetration and integration tests by those companies wishing to do their own diligence.

1.3 Self-assessment

Twice per year we review the latest version of the Minimum Viable Secure Product[7] document and update our own documentation to ensure compliance with the latest test security standards.

[2] Minimum Viable Secure Product: https://mvsp.dev/mvsp.en/
[3] Minimum Viable Secure Product, Frequently Asked Questions: https://mvsp.dev/questions/
[4] Vendor Security Model Contract: https://github.com/dropbox/vsmc
[5] VSAQ: Vendor Security Assessment Questionnaire: https://github.com/google/vsaq
[6] StatusGator Vulnerability Disclosure Policy: https://statusgator.com/security
[7] Minimum Viable Secure Product: https://mvsp.dev/mvsp.en/

1.4 External testing

Beginning in 2024, StatusGator will contract with a third-party security vendor to perform comprehensive penetration testing on our systems.

1.5 Training

All StatusGator employees and contractors undergo annual comprehensive Cybersecurity Awareness training and role-specific training.

1.6 Compliance

StatusGator complies with all local and international laws and privacy requirements. We provide compliance documentation such as Voluntary Product Accessibility Template (VPAT) to those customers that require it.

1.7 Incident handling

StatusGator maintains an incident response policy for both performance and uptime-impact incidents as well as security and privacy breaches. In the event of a breach, our policy requires that we notify affected customers within 72 hours of the discovery of any data leakage.

In addition, our notification template includes contact information (phone and email), a brief technical analysis and impact explanation, and a remediation plan with timelines and milestones.

1.8 Data handling

StatusGator ensures that all media is sanitized with processes based on NIST SP 800-88. Our PaaS cloud vendor follows even stricter requirements for hardware sanitization.

2. Application design controls

2.1 Single Sign-On

StatusGator allows SAML-based Single Sign-On (SSO) on all multi-user plans. We support all providers that allow SAML 2.0 authentication and provide vendor-specific documentation for the most common cloud authentication providers.

2.2 HTTPS-only

StatusGator does not permit any HTTP-only connections on any of its domains or any of the status pages it hosts on behalf of customers – we require HTTPS in all cases and at all times. We redirect any insecure HTTP request to an HTTPS request.

We send a strict-transport-security header with all requests and include a max-age of 63072000 seconds (2 years). We also include the includeSubDomains directive to ensure no *.statusgator.com can be served without HTTPS.

In addition, we monitor SSL certificate expiration and validity using TrackSSL[8].

2.3 Security Headers

Some StatusGator products are specifically designed to be embedded as iframes in other pages and those pages have permissive X-Frame-Options headers to allow embedding. All other pages use more restrictive X-Frame-Options headers with the SAMEORIGIN option.

2.4 Password policy

- We do not limit the permitted characters that can be used for characters.
- All passwords must be between 8 and 64 characters.
- We have no secret questions for password resets.
- We require email notification for all password change

[8] SSL Certificate Expiry Monitoring: https://trackssl.com/

requests.
- A password is required during authenticated change of passwords.
- We store all passwords in a hashed and salted CPU-hard one-hash hash function, bcrypt.
- After 5 failed authentication requests, users are locked out and notified via email.

In addition, StatusGator provides OTP-based two-factor authentication on all plans at no cost. To provide the most secure solution, we do not offer an SMS option for 2FA.

2.5 Security libraries

All of our infrastructure heavily relies on open source frameworks and libraries such as Ruby on Rails, to which we delegate the enforcement of input validation and sanitization.

2.6 Dependency Patching

We aggressively apply security patches and version upgrades to all levels of our stack. Most of our infrastructure is hosted on managed Platform-as-a-Service providers such as Heroku (by Salesforce) and they have robust handling of OS-level patches. For pieces of our infrastructure that are self-managed we have monthly tasks to ensure all our systems are appropriately patches. At the software level, use automation tools such as Dependabot[9] to protect against supply chain vulnerabilities.

2.7 Logging

We have extensive logging at several layers:

- Application-level logging storing key events.
- Database-level logging storing a history of changes to most tables.
- Infrastructure-level logging storing IP addresses and timestamps of actions performed.

[9] Keeping your supply chain secure with Dependabot: https://docs.github.com/en/code-security/dependabot

This ensures that all read, write, and delete operations are logged across system objects and that security changes including security system disabling is properly logged and audited.

2.8 Encryption

We use all modern means of encryption to store sensitive data at rest and in transit.

3. Application implementation controls

3.1 List of data

StatusGator processes very limited sensitive data: API tokens for customers that use our Private Status Ingestion feature and salted, hashed passwords for user accounts. Nothing more.

3.2 Data flow diagram

We maintain an updated data flow diagram for internal use and make it available to select customers upon request.

3.3 Vulnerability prevention

StatusGator has a robust system of code reviews in place to ensure high quality code and to limit vulnerabilities. In addition to human review, we use automated static analysis tools to catch security vulnerabilities before they are merged to production.

3.4 Time to fix vulnerabilities

We produce and deploy patches to address application vulnerabilities that materially impact security within 30 days of discovery. Our Platform-as-a-Service provider, Heroku, also aggressively maintains systems for security and performance.

3.5 Build process

Our build process is SLSA Level 1 compliant and is fully scripted and automated. We deploy to production an average of 8 times every day of the week, which is a testament to our aggressive automation and review process.

4. Operational controls

4.1 Physical access

Because StatusGator does not host any of our own infrastructure, we rely on the physical access controls of our cloud vendors. Our current providers all have extensive physical access controls:

- Heroku[10]
- Amazon Web Services[11]
- DigitalOcean[12]

4.2 Logical access

Access to production and customer data is severely restricted. Only a few specific StatusGator employees have access to customer information for the purposes of debugging customer integrations if, and only if, that is requested.

4.3 Subprocessors

Our Privacy Policy details our subprocessors.

4.4 Backup and Disaster recovery

In addition to our own backups to third-party vendors, StatusGator relies on the backup, disaster recovery, and

[10] Heroku Security: https://www.heroku.com/policy/security
[11] AWS Security: https://aws.amazon.com/compliance/data-center/controls/
[12] DigitalOcean Security: https://www.digitalocean.com/security

redundancy policies, products, and features of our cloud providers:

- Heroku
- Amazon Web Services
- DigitalOcean

statusgator

Nimble Industries, Inc.
1244 S. Evergreen Dr.
Phoenixville, PA 19460
hi@statusgator.com