Introduction

ServiceTitan is committed to resolving security vulnerabilities quickly and carefully. We take the necessary steps to minimize customer risk, provide timely information, and deliver vulnerability fixes and mitigations required to address security threats in our offerings.

ServiceTitan is committed to following the Carnegie Melon Coordinated Vulnerability Disclosure (CVD) for externally reported vulnerabilities. This process intends to minimize the harm to society posed by vulnerable products. We work closely with researchers who communicate vulnerabilities to us.

How to report a security vulnerability

If you believe you have found a vulnerability in a ServiceTitan product, cloud service, or IT infrastructure that has not been resolved, please contact security@servicetitan.com. To expedite verification of your finding, please provide the following information in your initial communication:

- Product name and version number, or URL
- Date the vulnerability was observed
- Description of the vulnerability
- Instructions to duplicate the vulnerability (this can be written steps, a video, or a set of screen captures detailing the proof of concept)
- Your name and company (if applicable)
- Your preferred contact information (email, phone, anonymous)
- Your PGP public key to allow for encrypted communication (if available)

The ServiceTitan will confirm receipt of your report within three business days. We will work with internal teams to verify the finding and respond in a timely manner with an update or request for additional information.

PGP key details

We encourage finders to use encrypted communication channels to protect the confidentiality of vulnerability reports using our PGP public key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEW8ZDbhYJKwYBBAHaRw8BAQdAEdrHONMoxiQjPogBKQfYslFPxvjKmF2Vnx+D
```

```
da2AQWq0PVNlcnZpY2VUaXRhbiBJbmZvcm1hdGlvbiBTZWN1cml0eSA8c2VjdXJp
dHlAc2VydmljZXRpdGFuLmNvbT6IlgQTFggAPhYhBCtyWJSogqCbyc9VeFzO1yYx
po/fBQJbxkNuAhsDBQkDw6pCBQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEFzO
1yYxpo/fZKsA/RdoNKsL9JmNr8oJOnxqnZAaoF2XPpHMLxzVSAfILcnpAP4m6r1D
WytmEmjsbT56osCqtbv1ua56BVia2WcKoUaUAbg4BFvGQ24SCisGAQQBl1UBBQEB
B0BJGQ9XP+CwYXF+pgwcQTf0in5Xta1uh1KVKmzVs9csNgMBCAeIfgQYFggAJhYh
BCtyWJSogqCbyc9VeFzO1yYxpo/fBQJbxkNuAhsMBQkDw6pCAAoJEFzO1yYxpo/f
dsMA/3tAQLHZvzJkSIN7dJSCpwCqKbHeXH/fWj8l4fbv/q3bAQDvBIGFM76KR2jo
BBO1/Z0G91U+sAgyj9OQflO80DLdDQ==
=2J5C
-----END PGP PUBLIC KEY BLOCK-----
```

Mitigation and remediation of finding

If the submitted finding is confirmed as valid, ServiceTitan will move forward with providing remediation or mitigation of the issue according to the impact and severity of the finding. The ServiceTitan security team will keep the reporter of the vulnerability up-to-date on progress until the issue has been addressed.

Conclusion

ServiceTitan is committed to addressing and resolving any security vulnerabilities that manifest in our software. We will work with finders to review, validate, and mitigate any security issues that are discovered and validated.