NoodleTools, Inc.

Update on Limited Data Breach - February 15th, 2024

Summary

Between February 6 and February 12, 2024, fewer than 940 users were exposed to a phishing website that mimicked the NoodleTools login screen. A subset of those users entered their NoodleTools username and password on that screen, at which point their login information was collected, consisting of:

- NoodleTools username
- NoodleTools password

Importantly, this was caught by our team quickly and, after the initial analysis, we took the NoodleTools site offline to prevent exposure for users (see timeline below).

Scope of incident and notification to affected schools/persons

Fewer than 940 users across approximately 250 schools (on average 3 or 4 users at each) could have been exposed. In accordance with privacy laws requiring that all affected persons be notified within 24 hours, starting at 10:30 PM on February 12, 2024 **we sent an email to the NoodleTools administrator at each of those schools**, identifying each user account and a description of the breach. Clear instructions detailed the steps they needed to take to help their users log back in safely.

I did not receive an email. Was my school affected?

Most schools and districts were not notified with an email (we serve 10,000+ schools) because, based on our analysis of the phishing tactic, they were either not targeted or there was no data breach or risk for them. However, for full transparency, we're providing this additional summary report to update all schools and districts we serve.

Is there any external privacy risk?

If a compromised NoodleTools password has been reused on other websites, the user should change that password globally. None of the affected users had used an email as their username.

Is there any residual privacy risk in NoodleTools?

There is no remaining risk for affected users within NoodleTools. All passwords were reset and logic was added to prevent a password from being changed back to the compromised one. The database has been sanitized and protections have been added (refer to "Mitigation and protection" below).

Incident details

Between February 5 and February 10, 2024, a bad actor exploited vulnerable code to inject trojan projects into random user accounts. The injected project was constructed such that a recipient who subsequently logged in and viewed the project was redirected to a phishing web page that looked identical to the NoodleTools login screen. If the user then re-entered their NoodleTools username and password, that data was logged. The phishing web page was hosted on an external, compromised website.

Timeline and response

Monday, February 5th, 2024:

- Identified suspicious activity around “copy project to another user” API use
- Investigated and started monitoring this potential issue
- As of February 10th, escalated suspicious API use to a priority mitigation task

Monday, February 12th, 2024 (times in PST):

- 10:30 AM: First report of a user getting redirected to a phishing website
- 10:45 AM: Analysis connects incident to earlier suspicious API activity
- 11:00 AM: NoodleTools development team begins mitigation tasks
    - Technical analysis, attack vector revealed and analyzed
- 12:00 PM: Analysis of the scope and exposure risk
- 12:30 PM: Full removal of the vulnerable API, initial sanitization of the database
- 1:00 PM: Full-team discussion of the feasibility of hardening server security without downtime
- 1:30 PM: Decision to take the site offline to prevent any possible further exposure
- 1:45 - 8:45 PM: Server is offline for service
    - Further analysis of scope
    - Identification of specific set of individuals affected
    - Code changes and full sanitization
- 10:30 PM - 5:45 AM: Email notifications with details and instructions sent to every affected school

Mitigation and protection

As of 8:45 PM PST on February 12th, 2024, before restoring service, the following mitigations were in place:

- Passwords of potentially compromised accounts reset
- Code added to prevent return to original password
- “Copy project to another user” API disabled
- Trojan projects deleted
- Redirection vulnerability eliminated
- Database sanitized

Ongoing protection plan includes:

- Reassess all API security and rate-limiting settings
- Develop a secure alternative for copying a project
- Identify vulnerabilities continuously via security tools and scans (e.g., OWASP ZAP)
- For non-SSO customers, implement a more secure login and registration procedure
- Augment activity monitoring

Who should I contact if I have a question?

Importantly, the administrator at each affected school was contacted as of 2/24/2024, and we continue to assist them individually as needed. If you have an urgent question regarding privacy, email privacy@noodletools.com.