April 1, 2026

5 min read time

osTicket timing vulnerability: Understanding the risk

Written by: Ruben Ferreira - Cyber Security Consultant

os ing side-channel
er 6-26895

Su

CS rsions 1.18.2 and below, tracked under CVE-2026-26895. osTicket is an open-source support ticket

system designed to help organisations manage customer service and IT support requests efficiently. It provides a centralised platform where users can submit tickets via email, web forms, or phone, whilst support teams can track, prioritise, and resolve issues accordingly. The vendor has released a fix addressing the reported vulnerability, and version 1.18.3 is no longer affected.

Technical details

A vulnerability has been identified within the /pwreset.php page of the osTicket application. This issue manifests only after the SMTP (Simple Mail Transfer Protocol) email service has been configured and is not present prior to its setup. The vulnerability presents itself as a significant discrepancy in server response times when processing password reset requests for existing usernames compared to non-existent ones. This timing discrepancy enables an attacker to perform user enumeration via brute force, as valid usernames can be inferred based on response latency. Although the vulnerability does not directly expose credentials, it increases the risk of targeted attacks by allowing adversaries to compile a list of valid accounts.

Proof of concept:

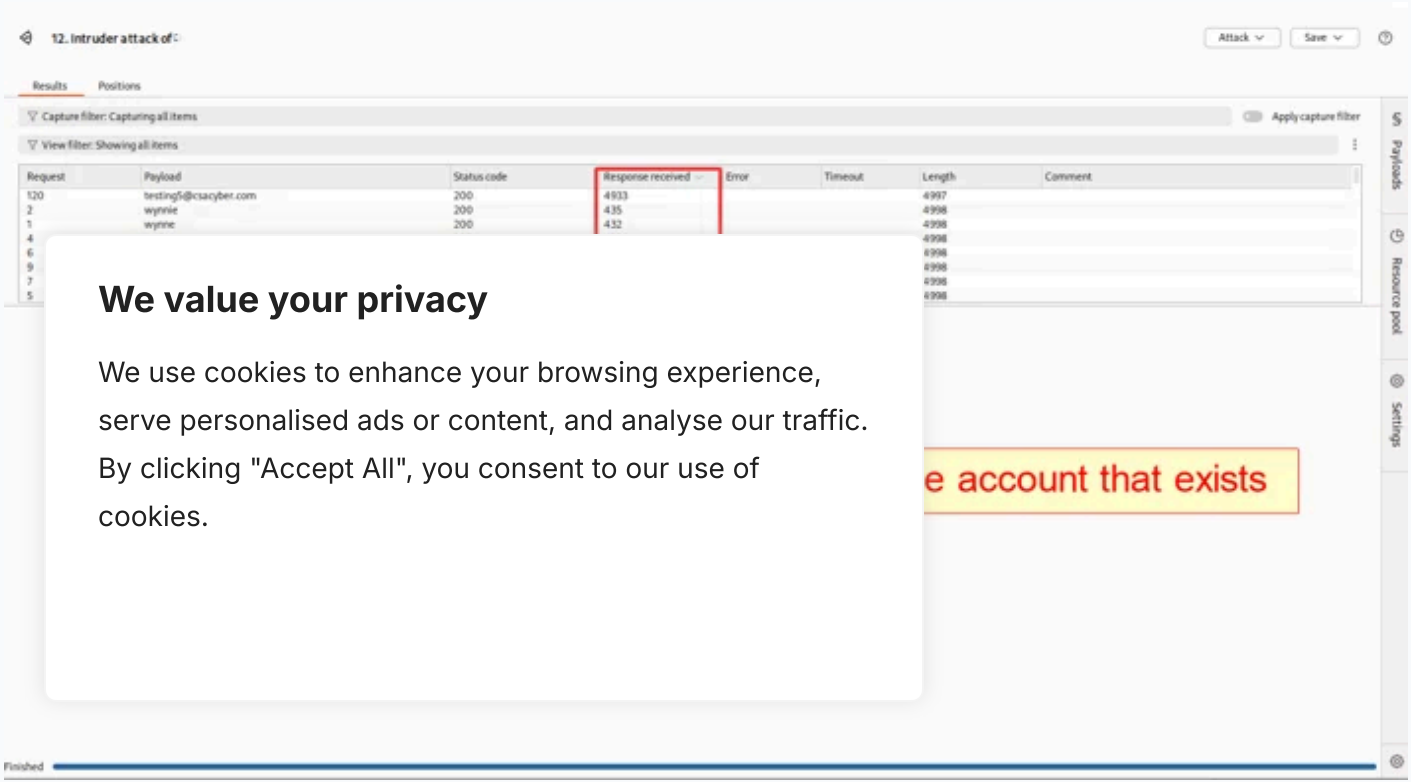

Figure 1: Burp Suite Intruder results demonstrating the response time discrepancy between valid and non-existent usernames.

Demonstrating impact

The impact of this vulnerability lies in its ability to enable user enumeration through measurable differences in server response times. When the SMTP (Simple Mail Transfer Protocol) service is configured, the password reset functionality on /pwreset.php behaves differently depending on whether the submitted username exists:

- **Valid username:** The application attempts to send a password reset email via SMTP (Simple Mail Transfer Protocol), resulting in a noticeably longer response time, typically several seconds.
- **Invalid username:** The application immediately returns an error without initiating email delivery, resulting in a considerably shorter response time, usually under one second.

This discrepancy allows an attacker to automate requests and infer valid usernames by analysing response latency. Once valid usernames have been identified, they can be leveraged for credential stuffing, phishing, or brute-force attacks, significantly increasing the risk of account compromise.

Example attack flow using Burp Suite

To the following steps:

1. **ompiles a list of potential us**

- s).
- doe).

Fo invalid usernames and one valid username.

2. Capture the password reset request

- Navigate to /pwreset.php and submit a password reset request.
- Intercept the request using Burp Proxy and forward it to Burp Intruder.

3. Configure Burp Intruder

- Set the payload position on the username parameter.
- Load the prepared username list into the payloads tab.
- Enable the response time column within the intruder results to measure latency.
- Select the sniper attack type for single-parameter testing.

4. Launch the attack

- Start the intruder attack to send sequential password reset requests for each username.
- Burp Suite will record response times for every request.

5. Analyse results and identify valid usernames review the intruder results as follows:

- Longer response time (e.g. 4–5 seconds) → Username exists (SMTP email triggered).
- Shorter response time (e.g. <1 second) → Username does not exist.

Compile the identified valid usernames for use in targeted attacks.

Ex

	Response Time
us	850 ms
us	870 ms
va	4,500 ms

Impact

This timing discrepancy allows attackers to enumerate valid accounts with a high degree of confidence. Once valid usernames have been identified, an attacker may proceed with:

- **Credential stuffing** using previously leaked passwords.
- **Phishing campaigns** targeting confirmed valid users.
- **Brute-force login attempts** against the application.

The consequences of these follow-on attacks can be severe for an organisation. A successful account compromise may result in:

- **Data breaches:** Exposing sensitive customer and employee data, potentially leading to regulatory penalties under frameworks such as GDPR or ISO 27001.
- **Reputational damage:** Loss of customer trust and confidence in the organisation's ability to safeguard their information.
- **Operational disruption:** Attackers gaining access to internal support systems may manipulate, delete, or exfiltrate tickets containing sensitive information.
- **Financial impact:** Costs associated with incident response, legal liability, regulatory fines, and potential compensation claims.

Remediation

Following responsible disclosure by Ruben Ferreira of Cyber Security Associates, the osTicket development team addressed the vulnerability in commit d832f24, released as part of version 1.18.3 on 15th January 2026. The fix was implemented by developer JediKev and is described as a "password reset hardening" measure.

The patch introduces a minimum response time on the /pwreset.php endpoint,
reg… within the system. This was
ac… ng microtime() and
en… ds, with a small random jitter
of … iming analysis. If the
re… e application deliberately
de… ng time. This ensures that
bo… onsistent and
indistinguishable response time, effectively eliminating the timing discrepancy that

enabled user enumeration.

As of version 1.18.3, osTicket is no longer vulnerable to this attack. Organisations running version 1.18.2 or below are strongly advised to upgrade immediately.

Disclosure timeline

15th January 2026: Vulnerability identified and reported to the vendor
15th January 2026: CVE request submitted
15th January 2026: A patch was released by the vendor to fix the vulnerability
24th February 2026: CVE ID CVE-2026-26895 received
1st April 2026: This blogpost published

The same-day turnaround between reporting, CVE submission, and patch release reflects a highly efficient and collaborative disclosure process. The vendor acted rapidly to validate the finding and deploy a fix.

Related Posts

You may also like this

Similar Articles

March 20, 2026 17 min read

Hybrid identity, fragmented security: How identity estates fuel modern breaches

In this article, I will cover why hybrid identities can lead to fragmented security and reduced...

Jack Gilmore

4 min read

Pr quantum readiness ca

Th htly so. Research such as Ma

February 2, 2026 11 min read

CVE-2026-21509 Analysis: The ghost in the document

In January 2026, Microsoft confirmed active exploitation of a high-severity zero-day,...

Steve Velcev

Est A Cyber provides cyber consultancy and te against the ever-changing cyber thr Military) and Commercially exp ations. Today our core services are based around a 24/7 Security Operations Centre (SOC) based in Gloucester.

News & Resources

Blog

Case Studies

Downloads & Reports

Webinars

Careers

Cyber Bundles (IT MSPs)

Quick Links

About Us

Certifications

Our Parent Company

Partners

Contact Us

Anti Bribery Policy

Complaints Policy

Corporate Social Responsibility Policy

Slavery and Human Trafficking Statement

NCSC CHECK Status Verification

CREST Approved Certification Verification

Contact Information

Un
Cyl
5 H

Un
Cyl
Uni

Ph
Em

United States of America
Cyber Security Associates Inc.
6010 W. Spring Creek Pkwy, Plano, Texas, 75024

Phone: +1 469 750 1695
Email: hello@csacyber.com