> Ghosts in the shell

.entry

Search

.entry
.articles
  .CVE-2025-63421
  .CVE-2025-61258
  .CVE-2023-27168
  .CVE-2023-27169
  .CVE-2023-27170
  .CVE-2023-27172
  .dllMemoryScanner
  .MessageBoxInjection
  .RtwqExecution
  .avEvasion

.CVE-2025-61258
Vulnerability Overview
Context
Outsystems overview
Technical description
Impact
Mitigation
Timeline
Disclosure
Credits
References

.CVE-2025-61258

Vulnerability Overview

Denial-of-service on Outsystems on-prem Platform Server.

Context

During a contracted penetration test on an Outsystems developed API, a denial-of-service vulnerability was discovered which impacted a wide range of components, branching from the API, webserver and outsystems dashboard, essentially affecting the whole outsystems **platform server**. This issue was discovered on **Outsystems Platform Server 11.18.1.37828** and allows attackers to cause a denial of service via crafted content-length value mismatching the body length.

Outsystems overview

To aid the reader, a small overview is provided:
Outsystems is a Portuguese unicorn company that developed and maintains a low-code development platform, providing tools for companies to develop, deploy and manage omnichannel enterprise applications.

Technical description

When assessing a given endpoint, specifically testing for HTTP request smuggling. A curious behaviour was observed when performing a POST request with a spoofed content length header, with a modified value higher than the actual body length.
So doing something like this:

```
POST /books/ HTTP/1.2
host: test.tld
content-length: 100
...

uuid=12332&author=john
```

Caused the server to hang indefinitely, the expected behaviour in this situation would be to timeout the request since the server never got the missing bytes specified in the request's header. Obviously the first thing that came to mind was to open a lot of paralel connections and see if the server would be able to keep up.

This is when the exploit formally materializes, by creating multiple concurrent HTTP connections using POST HTTP requests, in which the body's content is transmitted very slowly and in small blobs I was able to force the server to maintain multiple active connections and exhaust computational resources achieving a successful DoS attack. The attack afected everything from the API, to Outsystem's user dashboard and IIS static page. This type of denial of service is commonly called R.U.D.Y 'R U Dead Yet?' it's a low-and-slow denial attack, in which the attacker hunts for an endpoint that accepts

a POST request and then exhausts the server by keeping multiple connections tied up in a minimal bandwidth consumption session.

The attack can be replicated with a tool like slowhttptest, : `slowhttptest -c 10000 -B -o slowhttp -r 200 -u http://host.tld/endpointPostRoute`

During our tests, less than 500 simultaneous connections were sufficient to make the server unresponsive.

Root cause

We estimate the cause of this vulnerability lies in the default IIS webserver deployed as part of the outsystems plaftorm server stack.

Impact

This vulnerability has the potential to impact all outsystems applications deployed with the platform's server default IIS configurations. The exploit has a low complexity and is easily reproduced using multiple existing online tools, a single computer could deactivate a server. Without proper mitigation a vulnerable system is an easy target to decentralized versions of this exploit, since the attacker can escalate resources quicker than the victm. Simply increasing computational resources will not effectively solve the underlying problem.

CVE ID: CVE-2025-61258
CVSS 4 Base Score: 8,2
CVSS Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L
Affected Vendor: Outsystems
Affected Product: Outsystems Platform Server
Affected Version: 11.18.1.37828

Mitigation

No official fix or patch yet, although some hotfixes can be applied:

- Configure a hard timeout, cutting off lingering TCP and HTTP sessions after a sensible amount of time.
- Set a maximum number of concurrent connections allowed from a single source.
- Implement general brute-force attacks prevention measures.

Timeline

September 2025 - Vulnerability found and disclosed to customer September 2025 - Vulnerability submitted to mitre's CVE program December 2025 - Public Disclosure

Disclosure

Balwurk attempted to contact Outsystems through multiple channels through clients and partners, never receiving an official response indicating a fix or patch.

Credits

me

References

https://www.cloudflare.com/learning/ddos/ddos-attack-tools/r-u-dead-yet-rudy/
https://www.outsystems.com/

Site built with MkDocs and Terminal for MkDocs.