intruder

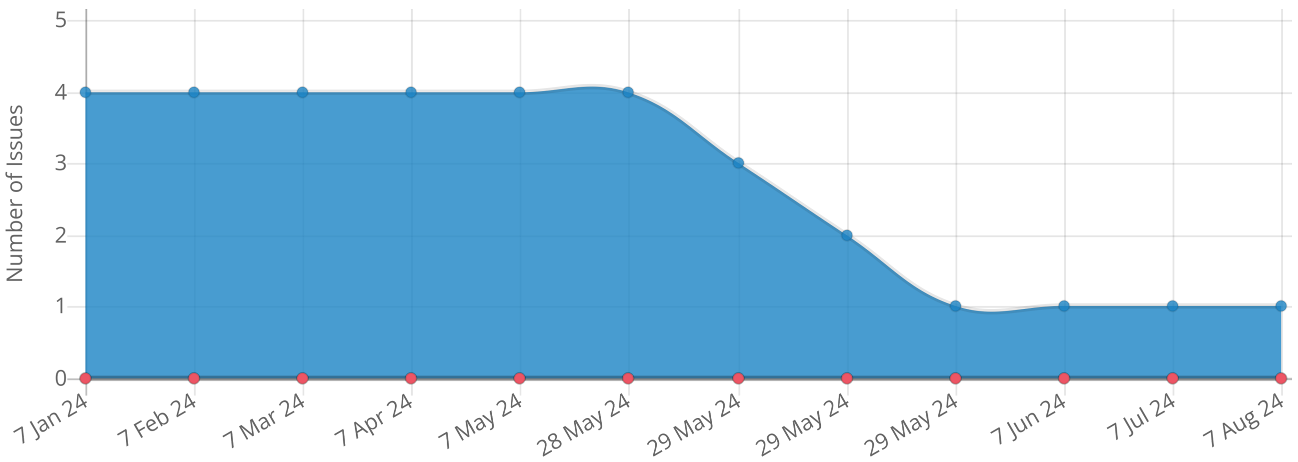
Scan Summary: **CloudRadial**
Targets: **2 targets scanned**
7 August 2024

Low
Threat Level

Low severity issues can not directly be exploited by an attacker, but may increase the ease of exploiting more severe issues in future. Fixing these issues may help protect against weaknesses that are not publicly known, or be used as one component in a highly targeted attack by the most sophisticated and well resourced attackers.

0	0	0	1
Critical issues	**High** issues	**Medium** issues	**Low** issue

Exposure over time



Differences since last assessment

New issues discovered		Previous issues remediated		Direction of travel
Critical	0	Critical	0	⬍ 0
High	0	High	0	⬍ 0
Medium	0	Medium	0	⬍ 0
Low	0	Low	0	⬍ 0

What we checked

Total checks	Targets	Issues discovered
14,286	2	1

Here are some examples of what we checked your targets and their reachable webpages for.

Vulnerable software & hardware

- Web servers, e.g. Apache, Nginx
- Mail servers, e.g. Exim
- Development software, e.g. PHP
- Network monitoring software, e.g. Zabbix, Nagios
- Networking systems, e.g. Cisco ASA
- Content management systems, e.g. Drupal, Wordpress
- Other well-known weaknesses, e.g. 'Log4Shell' and 'Shellshock'

Attack Surface Reduction

Our service is designed to help you reduce your attack surface and identify systems and software which do not need to be exposed to the Internet, such as:

- Publicly exposed databases
- Administrative interfaces
- Sensitive services, e.g. SMB
- Network monitoring software

Encryption weaknesses

Weaknesses in SSL/TLS implementations, such as:

- 'Heartbleed', 'CRIME', 'BEAST' and 'ROBOT'
- Weak encryption ciphers & protocols
- SSL certificate misconfigurations
- Unencrypted services such as FTP

Web Application Vulnerabilities

- Checks for multiple OWASP Top Ten issues
- SQL injection
- Cross-site scripting (XSS)
- XML external entity (XXE) injection
- Local/remote file inclusion
- Web server misconfigurations
- Directory/path traversal, directory listing & unintentionally exposed content

Information Leakage

Checks for information which your systems are reporting to end-users which should remain private. This information includes data which could be used to assist in the mounting of further attacks, such as:

- Local directory path information
- Internal IP Addresses

Common mistakes & misconfigurations

- VPN configuration weaknesses
- Exposed SVN/git repositories
- Unsupported operating systems
- Open mail relays
- DNS servers allowing zone transfer

As a **Pro** plan customer, you also have access to:

Emerging threats

The time between new vulnerabilities emerging and hackers exploiting them is now days, not weeks. For organizations who need a more mature approach to cyber security, our emerging threat scans detect critical threats to your systems without waiting for the next monthly check.

Internal checks

Your internal systems can also be hacked with a little extra effort, e.g. by an email or web page link that exploits known unpatched software or an employee's device. Our agent-based scanner can be installed on each machine you want to protect.

Issue Summary

Severity	Issue details
Low	**Strict Transport Security HTTP Header Not Set** Number of occurrences: 1

Issues

Strict Transport Security HTTP Header Not Set (Low)

Description

The server does not set a “Strict Transport Security” HTTP header in its response.

The HTTP Strict Transport Security policy defines a timeframe within which a browser must connect to the web server via HTTPS. The header adds additional protection against MitM (Man-in-the-Middle) attacks by instructing the user's web browser not to connect to the server unless it is done so over HTTPS with a valid certificate. This helps prevent an attacker in a MitM position from tricking the user into connecting to an attacker controlled server which is impersonating the targeted site.

Remediation Advice

Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]

The parameter max-age gives the time frame for requirement of HTTPS in seconds and is recommended to be set for at least several months, with 90 days being a minimum (ie. 7776000 seconds). The flag includeSubDomains defines that the policy should also apply for sub domains of the sender of the response.

For example, the following lines can be added to an Apache configuration file:

```
Header set Strict-Transport-Security "max-age=7776000"
Header append Strict-Transport-Security includeSubDomains
```

Occurrences

	First seen
api.us.cloudradial.com : 443 (tcp)	2023-02-25 21:47:01 UTC

Scan Info

Targets included in this scan

demo.us.cloudradial.com	api.us.cloudradial.com

Scan timings

This scan ran from 2024-08-07 00:01:09 UTC to 2024-08-07 07:31:53 UTC.

About us

Company

Intruder Systems Ltd is an independent security advisory company, specialising in providing continuous security monitoring for internet-facing web applications and infrastructure.

Security Team

Our consultants have delivered work for government agencies, international financial institutions, and global retail giants.

Credentials

Intruder is a member of CREST

Intruder is a CREST accredited Vulnerability Assessment service

Monitored by Drata for SOC 2 compliance

Intruder is a member of the Cyber-security Information Sharing Partnership

Intruder is Cyber Essentials certified.

GCHQ Cyber Accelerator Alumni

Compliance

Our reports are ISO 27001 and SOC 2 compliance ready.

Contact

contact@intruder.io

www.intruder.io

twitter.com/intruder_io

linkedin.com/company/intruder