

# Affected Items Report

Acunetix Security Audit

30 September 2019

# Selected vulnerabilities

---

## Scan details

---

Scan information	
Start url	https://observatory.mozilla.org/
Host	https://observatory.mozilla.org/

## Threat level


---

### Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

## Alerts distribution

---

Total alerts found	1
 High	1
 Medium	0
 Low	0
 Informational	0

## Affected items

<b>Web Server</b>	
<b>Alert group</b>	<b>nginx Integer Overflow</b>
<b>Severity</b>	High
<b>Description</b>	A security issue was identified in nginx range filter. A specially crafted request might result in an integer overflow and incorrect processing of ranges, potentially resulting in sensitive information leak (CVE-2017-7529). When using nginx with standard modules this allows an attacker to obtain a cache file header if a response was returned from cache. In some configurations a cache file header may contain IP address of the backend server or other sensitive information. Besides, with 3rd party modules it is potentially possible that the issue may lead to a denial of service or a disclosure of a worker process memory.
<b>Recommendations</b>	Upgrade nginx to the latest version or apply the patch provided by the vendor.
<b>Alert variants</b>	
<b>Details</b>	Current version is : nginx/1.10..

## Scanned items (coverage report)

---

<https://observatory.mozilla.org/>