

Readiness report

The Arabian Gulf against exploited vulnerabilities

Census of 23 October 2026

What the public websites of the six states announce about their software, held against CISA's catalogue of exploited vulnerabilities and against the support cycles their makers publish.

Key figures

84.8% of live domains answered with their first page
10,101 / 11,912

55.3% of the sites announcing a full Apache HTTP Server version
announce one affected by CVE-2024-38475
68 of 123 announcing a full version

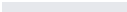
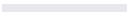
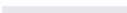
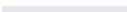
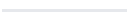
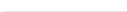
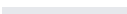
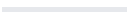
89.5% of the sites announcing a nginx version run one past its support
375 of 419 announcing a version

31.8% of the sites read announce the version of at least one piece of software
3,208 of 10,101 whose first page was read



Exploited vulnerabilities

Every vulnerability CISA has added to its catalogue of exploited vulnerabilities that affects software announced from outside, newest first, with the share of sites announcing an affected version among the sites that announce a version.

Share	Vulnerability	Affected of announcing	Catalogued
55.3% 	Apache HTTP Server CVE-2024-38475 Apache HTTP Server Improper Escaping of Output Vulnerability	68 / 123	1 May 2025
0.4% 	PHP CVE-2024-4577 PHP-CGI OS Command Injection Vulnerability Used in ransomware campaigns	4 / 1,097	12 June 2024
0.0% 	OpenSSL CVE-2014-0160 OpenSSL Information Disclosure Vulnerability	0 / 32	4 May 2022
0.3% 	PHP CVE-2012-1823 PHP-CGI Query String Parameter Vulnerability	3 / 1,097	25 March 2022
0.0% 	Drupal CVE-2020-13671 Drupal core Un-restricted Upload of File	0 / 65	18 January 2022
0.0% 	Apache HTTP Server CVE-2021-42013 Apache HTTP Server Path Traversal Vulnerability Used in ransomware campaigns	0 / 123	3 November 2021
0.0% 	Apache HTTP Server CVE-2021-41773 Apache HTTP Server Path Traversal Vulnerability Used in ransomware campaigns	0 / 123	3 November 2021
8.1% 	Apache HTTP Server CVE-2019-0211 Apache HTTP Server Privilege Escalation Vulnerability	10 / 123	3 November 2021
0.0% 	Drupal CVE-2018-7600 Drupal Core Remote Code Execution Vulnerability Used in ransomware campaigns	0 / 87	3 November 2021
0.4% 	Microsoft IIS CVE-2017-7269 Microsoft Windows Server Buffer Overflow Vulnerability	2 / 539	3 November 2021

And 7 more in Apache Tomcat and Joomla, which no site announces a full version of, so they are not measured yet.

Software past its support

Among the sites that announce the version of their software, the share running a version its maker no longer supports according to endoflife.date, so it receives no security patches.

Share	Software	Past support of announcing	Most common cycles
0.1%	WordPress	2 / 1,448	7.1 · 7.0 · 6.9
27.9%	PHP	306 / 1,097	8.3 · 8.2 · 7.4
3.9%	Microsoft IIS	21 / 539	10.0 · 8.5 · 7.5
89.5%	nginx	375 / 419	1.29 · 1.24 · 1.18
2.2%	Apache HTTP Server	3 / 135	2.4 · 2.2
12.5%	Drupal	13 / 104	7
75.0%	OpenSSL	24 / 32	1.0.2 · 1.1.1 · 3.5

What sites announce

Only what a site writes about itself in the headers of its first page or in its generator tag is measured, so the figures are a floor, and sites behind a front such as Cloudflare do not announce their server.

79.4%	Announce their server	8,025 / 10,101
31.8%	Announce a software version	3,208 / 10,101
27.2%	Announce their content system	2,744 / 10,101
37.8%	Behind a front that hides the server	3,819 / 10,101

CIS Controls in the Arabian Gulf

Each figure is the share meeting the visible evidence, and it does not mean the safeguard is met, since most of what it asks happens inside and cannot be seen from outside.

Share	Visible evidence	Meeting of measured
9.5 Implement DMARC Implementation Group 2		
18.9%	DMARC enforced	2,250 / 11,908
69.8%	SPF in place	8,312 / 11,907
3.10 Encrypt Sensitive Data in Transit Implementation Group 2		
92.0%	Valid HTTPS	9,303 / 10,117
18.6%	HSTS for a year or more	1,884 / 10,117
86.5%	TLS 1.3 supported	8,750 / 10,117
67.8%	No TLS 1.0 or 1.1	6,656 / 9,817
52.2%	Post quantum ready	5,280 / 10,111
0.5%	MTA-STS enforced	50 / 9,338
16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities Implementation Group 2		
2.1%	security.txt published	214 / 10,109
2.2 Ensure Authorized Software is Currently Supported Implementation Group 1		
77.0%	Announce a version still supported	2,391 / 3,106
7.4 Perform Automated Application Patch Management Implementation Group 1		
71.9%	On the latest release of their support cycle	2,232 / 3,106
7.7 Remediate Detected Vulnerabilities Implementation Group 2		
95.8%	Announce no version hit by an exploited vulnerability	1,711 / 1,786

CIS Controls® by the Center for Internet Security, Inc. Safeguard numbers, titles and Implementation Groups are used as CIS publishes them, unchanged, under CC BY-NC-ND 4.0.

Method and limits

The first page of every live domain is requested once, as any browser would, and its Server and X-Powered-By headers and the generator tag in its first 64 kilobytes are read, and nothing else is asked of the site.

The vulnerabilities come from CISA's catalogue of exploited vulnerabilities, the affected version ranges from NVD and the support cycles from endoflife.date, and all three are refreshed with every measurement.

It is measured after every weekly issue and within a day of a new entry for visible software, no domain is named and the states are never ranked.

A site can announce a version older than its code when its distribution backports the fixes, as Red Hat and Debian do, and it can announce only its major, in which case it is counted only when every version under it is affected or none is, so the share measures what a site announces, not exactly what runs inside it.

Each state has its own figures on its own page of the site, never set beside another, and no domain is named.

Sources

CISA Known Exploited Vulnerabilities catalogue · Read on 23 October 2026 cisa.gov/known-exploited-vulnerabilities-catalog

NVD, the National Vulnerability Database · Read on 23 October 2026 nvd.nist.gov

Support cycles on endoflife.date · Read on 23 October 2026 endoflife.date

How to cite

Ali AlEnezi (2026). Gulf Cybersecurity Baseline, readiness report, census of 23 October 2026. <https://gbaseline.3li.info/en/readiness/report/>

علي العنزي (2026) خط الأساس الخليجي للأمن السيبراني تقرير الاستعدادية لقياس 23 أكتوبر 2026 على [/https://gbaseline.3li.info/readiness/report](https://gbaseline.3li.info/readiness/report)