

Port Number	Protocol	Services	Recommended Action
22	tcp	ssh	Update firewall rules or apply security patches
25	tcp	smtp	Update firewall rules or apply security patches
53	tcp	domain	Update firewall rules or apply security patches
80	tcp	http	Update firewall rules or apply security patches
110	tcp	pop3	Update firewall rules or apply security patches
443	tcp	http	Update firewall rules or apply security patches

- High: 27

i. Vulnerability Summary: Missing Anti-clickjacking Header

ii. Risk Rating: Medium

iii. Confidence Rating: Medium

iv. Description: The response does not include either Content-Security-Policy with 'frame-and

v. Details to Reproduce the Instance: No instances found for the alert.

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism w

v. Details to Reproduce the Instance: No instances found for the alert.

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism w

v. Details to Reproduce the Instance: No instances found for the alert.

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism w

v. Details to Reproduce the Instance: No instances found for the alert.

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosni

v. Details to Reproduce the Instance: No instances found for the alert.