Remediation Guidance Report SAMPLE

PentaTrail

Domain example.co.jp · Generated 2026-07-06 · Order By threat exposure risk (TER), highest first

This document is a sample built from fictitious data for "Sample Trading Co., Ltd." It does not describe any real organisation.

AI remediation guidance summary

S 2 | A 2 | B 2 | C 1

Severity legend: S A B C D

S Apache HTTP Server 2.4.49

Affected hosts 2 · CVE 2

Impact

A path normalisation flaw allows access to files outside the published directory. Depending on the configuration, programs on the server can be executed from outside. Exploitation of this component has been confirmed in the wild.

Remediation

Update to 2.4.51 or later. If you run a distribution build, moving to a release that carries the corresponding patch has the same effect. Apache must be restarted after the update.

Temporary Mitigation

If you cannot update immediately, set an explicit "Require all denied" for "/" in the Directory directive and allow only the paths you intend to publish.

Related CVEs

CVE-2021-41773 CVE-2021-42013

Affected hosts（2）

www.example.co.jp shop.example.co.jp

S OpenSSL 3.0.0

Affected hosts 1 · CVE 2

Impact

A buffer overflow in the handling of strings inside certificates means that, where client certificates are accepted, a connecting party may be able to disturb the process.

Remediation

Update to 3.0.7 or later. Applications that link OpenSSL statically must be rebuilt after the update.

Temporary Mitigation

Temporarily disabling client-certificate authentication removes exposure through this path.

Related CVEs

CVE-2022-3602 CVE-2022-3786

Affected hosts（1）

vpn.example.co.jp

A PHP 7.4.x (end of life)

Affected hosts 1 · CVE 1

Impact

This release has reached end of life, so fixes for future defects will not be provided. In the past, a defect allowing remote code execution under certain configurations was found here.

Remediation

Migrate to PHP 8.2 or later. The migration requires replacing deprecated functions and reviewing places where type handling has become stricter.

Related CVEs
CVE-2019-11043

Affected hosts（1）
api.example.co.jp

A nginx 1.18.0

Affected hosts 2 · CVE 1

Impact
A defect in the handling of name-resolution responses means that, where an upstream resolver is used, a crafted response may be able to disturb the process.

Remediation
Update to 1.20.1 or later. No configuration change is required.

Temporary Mitigation
If your configuration does not use the resolver directive, this path does not apply. If it does, point it only at resolvers you trust.

Related CVEs
CVE-2021-23017

Affected hosts（2）
www.example.co.jp api.example.co.jp

B Missing sender-domain authentication (SPF / DMARC)

Affected hosts 1

Impact
Recipients cannot tell whether mail claiming to come from this domain is genuine, which leaves room for messages impersonating your organisation.

Remediation
Publish an SPF record that permits only the servers you send from. Add DMARC with p=none as well, collect the reports on actual sending, and tighten the policy in stages.

Affected hosts（1）
mail.example.co.jp

B TLS certificate hostname mismatch

Affected hosts 1

Impact
The name on the presented certificate does not match the host being reached. Visitors see a browser warning, and once they grow used to warnings they can no longer tell a genuine site from a fake one.

Remediation
Reissue and install a certificate that covers this hostname. If the host answers to several names, include all of them in the certificate.

Affected hosts（1）
shop.example.co.jp

C Missing security headers

Affected hosts 2

Impact

Headers that switch on browser-side defences are absent. This does not cause harm on its own, but it widens the impact when combined with another defect.

Remediation

Set Content-Security-Policy and X-Content-Type-Options. Introduce Content-Security-Policy in Report-Only mode first and confirm the existing pages still render before enforcing it.

Affected hosts（2）

example.co.jp www.example.co.jp