METAPORT

.NET

Application Health Report: Hello World App

Generated on: **26/02/2026**
Prepared by: **Jane <jane.doe@acme.co>**
Report Status: **Final**

AT RISK

Projected Risk Horizon: application will remain at **AT RISK** in 30 days on Mar 28, 2026 if no action is taken beforehand.

End of life:	Security Vulnerabilities:	SSL Certificate:
IMMINENT	WARNING	OK

Contents

Executive Summary

The application **Hello World App** is built on .NET/NuGet and was last released to production on Feb 19, 2026. It's currently rated **AT RISK**.

Urgent work is required to ensure the application returns to a healthy state which reduces business risk for the customer in the event of an incident.

The longer the application remains in this state, the likelihood of a security incident increases, which may result in a breach of Support or Maintenance Agreement(s).

The application will remain at **AT RISK** in 30 days on Mar 28, 2026 if no action is taken beforehand.

Risk Summary

The application currently has **0** issue(s) rated **CRITICAL**, **1** issue(s) rated **IMMINENT**, and **1** issue(s) rated **WARNING**.

There is currently business and operational risk for this application when operating in a production environment which should be remediated.

If not already, the effort required to remediate should be covered by a monthly Support or Maintenance Agreement or retainer contract. If a contract is not in place, time, budget, and resource is required on a time & materials basis to return the application to an **ON TRACK** state.

Issue	Severity	Risk Summary
End of life	IMMINENT	Not keeping on top of major software component upgrades can cause: • Software Supply Chain Failures • Authentication Failures • Software or Data Integrity Failures Which may lead to: • Possible data breaches • Possible service downtime • Possible defacement attacks • Hindered feature development and increased technical debt • Loss of business and/or reputation

Security Vulnerabilities	WARNING	Not securiing software components increases the potential for issues to arise related to: • Broken Access Control • Security Misconfiguration • Injection • Authentication Failures • Software or Data Integrity Failures • Mishandling of Exceptional Conditions Which may lead to: • Possible data breaches • Possible service downtime • Possible defacement attacks • Loss of business and/or reputation
SSL Certificate	OK	Expired SSL certificates are an immediate problem for users and may cause: • Authentication Failures • Cryptographic Failures Which may lead to: • Users unable to use the app • Users may see browser errors or warnings • User data is not protected in transit • Loss of business and/or reputation

Maintenance Summary

Dotnet 8 is due to go end-of-life in about 9 month(s). Version(s) 9, 10 are available. An upgrade project and budget should already be planned.

There are 0 security vulnerabilties rated with a "High" or above severity.

There are 0 security vulnerabilties rated with a "Medium" severity.

There is 1 security vulnerability rated with a "Low" severity.

The SSL certificate is not currently due for renewal. It will expire in 140 days on Jul 17, 2026.

Recommendations Summary

Regardless of the existence or the severity of any issues, the following recommendations should be followed.

Issue	Recommendation
End of life	**Near Term:** Review the maintenance calendar, secure resource to estimate upgrade effort, open a ticket, and ensure timings and budgets are agreed. **Medium Term:** Also ensure a Metaport Policy is set-up to notify team members for End of life
Security Vulnerabilities	**Near Term:** Raise with development and security teams and open tickets as required. **Medium Term:** Ensure a Support or Maintenance Agreement is in place. Also ensure a Metaport Policy is set-up to notify team members for Security Vulnerabilities
SSL Certificate	**Near Term:** Raise with development or operations teams as soon as possible and open a ticket. **Medium Term:** Discuss auto-renewal options with technical teams and the customer as necessary. Also ensure a Metaport Policy is set-up to notify team members for SSL Certificate

Appendix

AT RISK This application needs urgent attention to remain secure. There are one or more high-severity issues which on their own increase risk from a range of network based attacks.

ATTENTION This application requires additional work to remain secure and keep security risk to a minimum. While the risk is not yet urgent, it pays to keep maintenance

efforts to a minimum.

ON TRACK This application is up-to-date. While there is no present risk, it still pays to keep maintenance efforts to a minimum and avoid Hello World App escalating to an AT RISK state.

Monitored Indicators

The report concerns itself with the following maintenance indicators which are used to calculate the health of Hello World App:

SSL certificate expiry date

SSL certificates encrypt data sent between a user's browser and Hello World App. Certificates have a finite life and need to be renewed. Automatic renewal is desirable, not always possible. The severity of this issue increases as expiry dates near.

End of life (EOL) expiry

Hello World App is built from individual software components so developers don't need to build things from scratch.

When a component is no longer supported by its maintainer, it is said to be "End of life". Without upgrade or replacement, the number of security vulnerabilties discovered increases over time, as does the complexity and expense of upgrading to the next version.

The severity of this issue is measured by the number of months until the expiry date.

Security Vulnerabilties

The number of global security incidents is growing in both number and severity. There are dozens of ways threat actors may gain unauthorised access to Hello World App for the purposes of defacement, denial of service, or data exfiltration for sale to the highest bidder.

The severity of this issue is measured by the number of security vulnerabilities rated "High" or above.

Note: Security vulnerabilities are all about context. The way in which a potentially vulnerable software component is used within Hello World App means it may or may not be exploitable. Developers therefore need to consult available documentation and triage

the issue before actioning any work.

Report generated automatically by Metaport.