Security Report

Dynamicweb Security Issue #6458

TECHNICAL DESCRIPTION

Version: 1.0

2022.01.24

LEGAL INFORMATION

CONTENTS

Contents

INTRODUCTION

What this document is about

This document describes a security issue in Dynamicweb.

Security issues are scaled by severance on a 4 step scale:

1. Critical
2. High
3. Medium
4. Low

This issue is categorized as ***CRITICAL***

Actions to remediate the issue is **absolutely required**.

Who this document is for

This document is for developers and technical personnel handling Dynamicweb solutions build on these versions of Dynamicweb.

- Dynamicweb 9.5.0 - 9.12.7 (Internal version 9.5+) with build date later than 28/8-2018

This security update is rated with a **critical** impact on security!
This security update is rated with a **medium** impact on personal data

1 SECURITY ISSUE

This security update addresses a vulnerability that makes an attacker able to get access to the administration of the Dynamicweb backend (/Admin) with administrative permissions. Using this access the attacker can get access to data about users, customers, orders and other information on the solution. The access can also be used for defacement or changing content on pages to use it for phishing attacks and other malicious behavior

The vulnerability is considered *Critical impact* for general website security.

The vulnerability is considered *medium impact* for disclosure of personal information as defined in GDPR regulations (Directive 95/46/EC).

This is a friendly report and the vulnerability has not been exploited. See section 1.2

For some organizations in the EU, or for organizations operating in the EU, this breach, if the solution is affected, might require a registration with the local authorities that requires a report of a data breach if it is assessed that this vulnerability has been exploited on or after May 25th, 2018. This can be verified by searching webserver log files. Consult your internal data policies or legal advisor weather it is required to file a report.

1.1 Affected and Non-Affected versions of Dynamicweb

Some versions of Dynamicweb is affected by this issues and others are not.

1.1.1 Affected versions

The only affected versions are listed below

- Dynamicweb 9.5.*
- Dynamicweb 9.6.*
- Dynamicweb 9.7.*
- Dynamicweb 9.8.*
- Dynamicweb 9.9.*
- Dynamicweb 9.10.*
- Dynamicweb 9.12.*

1.1.2 Non-Affected versions

Versions not listed above is not affected by this issue – which means that solutions using the following versions do not need any additional action

- All versions of Dynamicweb 9 prior to version 9.5.0
- All Dynamicweb 6, 7 and 8 versions
- Dynamicweb 10 pre
- Dynamicweb installations without a public /Admin folder

1.1.3 Fixed versions

These releases of Dynamicweb will contain hotfix for the vulnerability in question. All these are new releases for each Dynamicweb minor after 9.5.0 that will contain the fix.

An upgrade to one of these versions is required, alternatively a standalone fix can be applied on existing installations without upgrading – see section 1.3 “Patching installations”

- Dynamicweb 9.5.10
- Dynamicweb 9.6.17
- Dynamicweb 9.7.9
- Dynamicweb 9.8.13
- Dynamicweb 9.9.10
- Dynamicweb 9.10.20
- Dynamicweb 9.12.9
- Dynamicweb 9.13.0

1.2 Vulnerability information

A malicious attacker can target a part of the backend of Dynamicweb residing under /admin and by submitting specific values in a request, the attacker is allowed to create a user in Dynamicweb.

The created user will have administrative privileges and can be used to gain access to the backend as a backend administrator.

The access can be used to obtain all the information in the solution – i.e., content, product data, user information, order history etc.

Additionally, the access can also be used to alter the content and settings of the installation and change i.e., content on published pages, change prices, create discounts etc.

Also, templates can be changed or uploaded, and scripts can be added to templates to setup phishing pages or place malicious code for later exploitation.

Source of vulnerability

This issue has been reported by a security company that has assessed Dynamicweb 9.12.6 and discovered the issue by exploring decompiled source code of Dynamicweb.

This means that it is a friendly discovery of the security issue and it has not been found through a malicious exploit by hackers.

The issue is currently unknown publicly and has – to our knowledge – not have been exploited.

We have not received any reports where unauthorized access to Dynamicweb has happened.

1.3 Patching installations

Depending on which version of Dynamicweb you have and where it is hosted, there are different paths to getting patched.

- Solution hosted by Dynamicweb
- Solutions NOT hosted by Dynamicweb – using upgrade
- Solutions NOT hosted by Dynamicweb - using standalone patch

Solutions hosted by Dynamicweb will be patched by Dynamicweb Operations. The patch has been applied on January 21st late in the evening.

All other installation types need to be updated manually by following one of the following approaches

1.3.1 Solutions patched by Dynamicweb

These solution types that are managed and hosted by Dynamicweb have been patched by Dynamicweb Operations

- Dynamicweb Cloud
- Dynamicweb Free, Express and Standard

1.3.2 Solutions *not* hosted by Dynamicweb - upgrade

Upgrade your Dynamicweb installation to the latest hotfix on your minor. If the version of the current installation is 9.5.*, update to 9.5.9 below, if the current installation is 9.6.* update to 9.6.16 etc.

- Dynamicweb 9.5.9
- Dynamicweb 9.6.16
- Dynamicweb 9.7.8
- Dynamicweb 9.8.11
- Dynamicweb 9.9.8
- Dynamicweb 9.10.18
- Dynamicweb 9.12.8

Dynamicweb 9.13.0 released on January 25th 2022 is not affected and contains the fix already.

1.3.3 Solutions *not* hosted by Dynamicweb – standalone patch

Solutions that cannot be upgraded can be patched by adding an assembly to the solutions /bin folder.

The assembly (dll) contains a general implementation that is not targeting a specific version of Dynamicweb, but will intersect the malicious attack and block the request.

Download the zip from https://doc.dynamicweb.com/downloads/ and unzip it to a local directory

Copy the `DynamicwebSoftware.Security.DevOps6458.dll` to the solution **/bin** folder in the root of the solution.

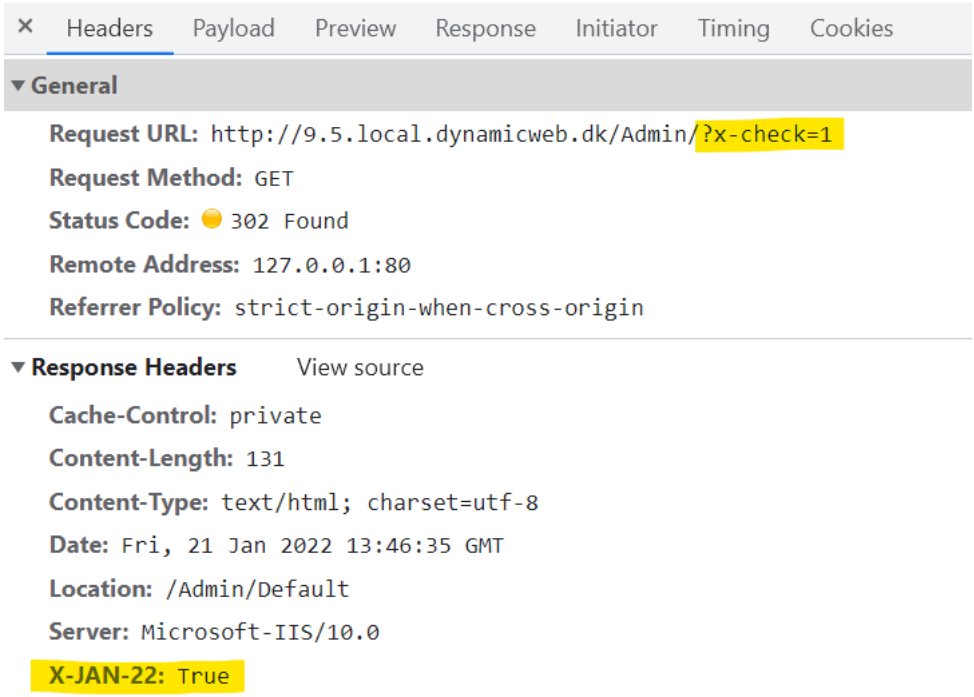
To verify that the patch is applied to a solution a request to the /admin can be made and by inspecting the response header, it can be detected if this assembly is applied.

To check, add x-check=1 either as a request-header or querystring

/admin?x-check=1

If the response contains a `x-jan-22: true` header, the solution has been patched.

This can be used for automation of checks in hosting environments.



2 Legal Disclaimer

The information contained in this document is for general guidance on matters of interest only. The application and impact of laws can vary widely based on the specific facts involved.

As such, it should not be used as a substitute for consultation with professional legal or other competent advisers.

Before making any decision or taking any action, you should consult a GDPR legal professional.

This document is based on our views and interpretation of GDPR based on our work with our advisors.