


[skip to content](#)
[Back to GitHub.com](#)



[Security Lab](#)
[Bounties](#) [Research](#) [Advisories](#) [Get Involved](#) [Events](#)

[Home](#) [Bounties](#) [Research](#) [Advisories](#) [Get Involved](#) [Events](#)
October 30, 2020

GHSL-2020-143: Arbitrary Code Execution in FastReports - CVE-2020-27998



[Jaroslav Lobacevski](#)

Summary

FastReports is vulnerable to arbitrary code execution because it compiles and runs C# code from a report template.

Product

[FastReports](#)

Tested Version

Master branch.

Details

Issue: [Compilation](#) of user supplied expressions into a .NET assembly.

While the dynamic data transformation into a compiled .NET code could be acceptable if the report template and the data from data source are trusted, the advertised [Online Designer demonstrates](#) that this assumption does not hold true.

Any user may run arbitrary remote code on the server by creating a new expression or editing an existing one into, for example `[System.String.Join(", ", System.IO.Directory.GetDirectories(@"c:/"))]`.

Side Note: The forward slash '/' is used instead of the back slash '\' because FastReports library fails to recognize a string literal if the last character is '\'.

After the user clicks `Preview` the code is executed on the server.

Impact

Arbitrary code execution on the report template processing host.

Remediation

The allowed expressions should be restricted to an acceptable subset. The compiled code should be run in a sandboxed process.

CVE

- CVE-2020-27998

Coordinated Disclosure Timeline

- 24/08/2020: Report sent to Vendor
- 26/08/2020: Vendor acknowledges
- 28/08/2020: Vendor implements a filtering to remediate the issue
- 07/09/2020: Vendor publishes an [announcement](#)
- 29/10/2020: CVE-2020-27998 got assigned

Resources

- The fix - <https://github.com/FastReports/FastReport/pull/206>
- Vendor advisories:
 - <https://opensource.fast-report.com/2020/09/report-script-security.html>
 - <https://fast-report.com/en/blog/360/show/>

Credit

This issue was discovered and reported by GHSL team member [@JarLob \(Jaroslav Lobačevski\)](#).

Contact

You can contact the GHSL team at securitylab@github.com, please include a reference to GHSL-2020-143 in any communication regarding this issue.

GitHub

Product

- [Features](#)
- [Security](#)
- [Enterprise](#)
- [Customer stories](#)
- [Pricing](#)
- [Resources](#)

Platform

- [Developer API](#)
- [Partners](#)
- [Atom](#)
- [Electron](#)
- [GitHub Desktop](#)

Support

- [Docs](#)
- [Community Forum](#)
- [Professional Services](#)
- [Status](#)
- [Contact GitHub](#)

Company

- [About](#)
- [Blog](#)
- [Careers](#)
- [Press](#)
- [Shop](#)



- © 2021 GitHub, Inc.
- [Terms](#)
- [Privacy](#)
- [Cookie settings](#)