

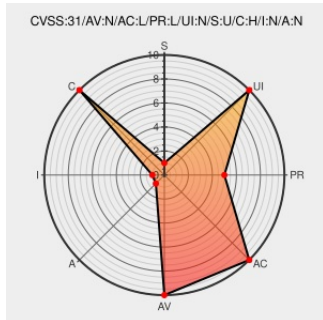


CVE-2020-35992

Published on: Not Yet Published

Last Modified on: 08/25/2022 08:45:00 PM UTC

CVE-2020-35992

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Prologue](#) from [Fiserv](#) contain the following vulnerability:

Fiserv Prologue through 2020-12-16 does not properly protect the database password. If an attacker were to gain access to the configuration file (specifically, the LogPassword attribute within appconfig.ini), they would be able to decrypt the password stored within the configuration file. This would yield cleartext credentials for the database (to gain access to financial records of customers stored within the database), and in some cases would allow remote login to the database.

CVE-2020-35992 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Financial Services Technology, Mobile Banking, Payments Fiserv	www.fiserv.com text/html	www.fiserv.com
GitHub - micahvandeusen/PrologueDecrypt	github.com text/html	github.com/micahvandeusen/PrologueDecrypt

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fiserv	Prologue	All	All	All	All
cpe:2.3:a:fiserv:prologue:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-35992 : Fiserv Prologue through 2020-12-16 does not properly protect the database password. If an attacker... twitter.com/i/web/status/1...	2022-08-23 02:09:05
 @JohnJasonFallow	New vulnerability on the NVD: CVE-2020-35992 ift.tt/JXKyBnP	2022-08-23 05:16:36
 @workentin	New vulnerability on the NVD: CVE-2020-35992 ift.tt/2rhUSgd	2022-08-23 05:40:52
 @vuldb	[Exploit] We have added entry VDB-206960 containing an exploit for CVE-2020-35992 vuldb.com/?id.206960	2022-08-23 05:49:19
 @xanadulinux	CVE-2020-35992 ift.tt/VYfRQkL	2022-08-23 05:52:38
 @doogsineerg	New vulnerability on the NVD: CVE-2020-35992 ift.tt/uLBkM48	2022-08-23 07:33:26
 @Har_sia	CVE-2020-35992 har-sia.info/CVE-2020-35992... #HarsialInfo	2022-08-23 18:26:03
 @threatmeter	CVE-2020-35992 Fiserv Prologue through 2020-12-16 does not properly protect the database password. If an attacker w... twitter.com/i/web/status/1...	2022-08-24 07:09:23
 @ColorTokensInc	Emerging Vulnerability Found CVE-2020-35992 - Fiserv Prologue through 2020-12-16 does not properly protect the data... twitter.com/i/web/status/1...	2022-08-25 21:12:15
 /r/netcve	CVE-2020-35992	2022-08-23 02:41:00

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)