



# CVE-2023-34366

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-34366
<b>State</b>	PUBLIC
<b>Assigner</b>	talos-cna@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-19 18:15:00 UTC
<b>Updated</b>	2023-10-25 14:30:00 UTC
<b>Description</b>	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Justsystems</a>	<a href="#">Easy Postcard Max</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Ichitaro 2021</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Ichitaro 2022</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Ichitaro 2023</a>	1.0.1.59372	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Ichitaro Government 10</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Ichitaro Government 8</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Ichitaro Government 9</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Ichitaro Pro 3</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Ichitaro Pro 4</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Ichitaro Pro 5</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Just Government 3</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Just Government 4</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Just Government 5</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Just Office 3</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Just Office 4</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Just Office 5</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Just Police 3</a>	-	All	All	All

Application	<a href="#">Justsystems</a>	<a href="#">Just Police 4</a>	-	All	All	All
Application	<a href="#">Justsystems</a>	<a href="#">Just Police 5</a>	-	All	All	All

## References

Reference	Source	Link	Tags
JVN#28846531: Multiple vulnerabilities in JustSystems products	MISC	<a href="#">jvn.jp</a>	
TALOS-2023-1758    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	<a href="#">talosintelligence.com</a>	
TALOS-2023-1758    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	<a href="#">www.talosintelligence.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

**Free CVE JSON API** [cve.report/api](#)

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