



# CVE-2021-35052

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

## Summary

<b>CVE</b>	CVE-2021-35052
<b>State</b>	PUBLIC
<b>Assigner</b>	vulnerability@kaspersky.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-11-23 16:15:00 UTC
<b>Updated</b>	2021-11-29 18:36:00 UTC
<b>Description</b>	A component in Kaspersky Password Manager could allow an attacker to elevate a process Integrity level from Medium to I

## Risk And Classification

**Problem Types:** CWE-269

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kaspersky	Password Manager	9.0.2	-	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_a	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_b	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_c	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_d	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_e	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_f	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_g	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_h	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_i	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_j	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_k	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_l	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_m	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_n	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_o	All	All
Application	Kaspersky	Password Manager	9.0.2	patch_p	All	All

Application	<a href="#">Kaspersky</a>	<a href="#">Password Manager</a>	9.0.2	patch_q	All	All
Application	<a href="#">Kaspersky</a>	<a href="#">Password Manager</a>	All	All	All	All

## References

Reference	Source	Link	Tags
List of Advisories	MISC	<a href="https://support.kaspersky.com">support.kaspersky.com</a>	
ZDI-21-1335   Zero Day Initiative	MISC	<a href="https://www.zerodayinitiative.com">www.zerodayinitiative.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[375996](#) WinRAR Multiple Remote Code Execution (RCE) Vulnerability

© [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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)