



# CVE-2020-7745

Published on: 10/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:53 PM UTC

## CVE-2020-7745

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

IS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N/E:H/RL:U/R



Certain versions of [Mintegraladsdk](#) from [Mintegral](#) contain the following vulnerability:

This affects the package MintegralAdSDK before 6.6.0.0. The SDK distributed by the company contains malicious functionality that acts as a backdoor. Mintegral and their partners (advertisers) can remotely execute arbitrary code on a user device.

CVE-2020-7745 has been assigned by [report@snyk.io](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.1 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>LOW</b>             | <b>HIGH</b>         | <b>NONE</b>         |

CVSS2 Score: **10 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                                                           | Tags                                                                                                                            | Link                                                     |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Remote Code Execution using Mintegral's MTGInvocationBoxing - YouTube | <a href="#">Exploit</a><br><a href="#">Third Party Advisory</a><br><a href="#">www.youtube.com</a><br><a href="#">text/html</a> | <a href="#">MISC www.youtube.com/watch?v=n-mEMkeoUqs</a> |

|                                                                                      |                                                                                              |                                                                         |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| SourMint: iOS remote code execution, Android findings, and community response   Snyk | <a href="#">Third Party Advisory</a><br><a href="#">snyk.io</a><br><a href="#">text/html</a> | <a href="#">MISC snyk.io/blog/remote-code-execution-rce-sourmint/</a>   |
| Malicious Package in mintegraladsk   Snyk                                            | <a href="#">Third Party Advisory</a><br><a href="#">snyk.io</a><br><a href="#">text/html</a> | <a href="#">MISC snyk.io/vuln/SNYK-COCOAPODS-MINTEGRALADSDK-1019377</a> |
| SourMint Malicious SDK Research write up   Snyk                                      | <a href="#">Broken Link</a><br><a href="#">snyk.io</a><br><a href="#">text/html</a>          | <a href="#">MISC snyk.io/research/sour-mint-malicious-sdk/%23rce</a>    |

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](mailto: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                                             | <a href="#">Mintegral</a> | <a href="#">Mintegraladsk</a> | All     | All    | All     | All      |
| Application                                             | <a href="#">Mintegral</a> | <a href="#">Mintegraladsk</a> | All     | All    | All     | All      |
| cpe:2.3:a:mintegral:mintegraladsk:*:*:*:*:iphone_os:*:* |                           |                               |         |        |         |          |
| cpe:2.3:a:mintegral:mintegraladsk:*:*:*:*:iphone_os:*:* |                           |                               |         |        |         |          |

Discovery Credit

Snyk Security Team

← Previous ID

Next ID→