



CVE-2018-20378

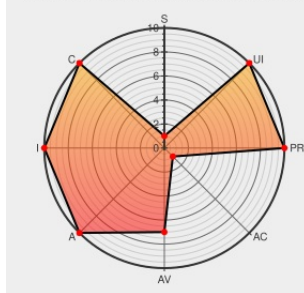
Published on: 03/29/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:37 PM UTC

CVE-2018-20378

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

CVSS:30/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Blue Sdk](#) from [Opensynergy](#) contain the following vulnerability:

The L2CAP signaling channel implementation and SDP server implementation in OpenSynergy Blue SDK 3.2 through 6.0 allow remote, unauthenticated attackers to execute arbitrary code or cause a denial of service via malicious L2CAP configuration requests, in conjunction with crafted SDP communication over maliciously

configured L2CAP channels. The attacker must have connectivity over the Bluetooth physical layer, and must be able to send raw L2CAP frames. This is related to L2Cap_HandleConfigReq in core/stack/l2cap/l2cap_sm.c and SdpServHandleServiceSearchAttribReq in core/stack/sdp/sdpserv.c.

CVE-2018-20378 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description

BlueSDK-advisory2018003 - OpenSynergy

Tags

Vendor Advisory

www.opensynergy.com

text/x-php

Exploit

Third Party Advisory

www.cymotive.com

application/pdf

Link

CONFIRM

www.opensynergy.com/news/security/bluesdk-advisory2018003/

MISC

www.cymotive.com/wp-content/uploads/2019/03/Hell2CAP-0day.pdf

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	Opensynergy	Blue Sdk	All	All	All	All
Application	Opensynergy	Blue Sdk	All	All	All	All
Application	Opensynergy	Blue Sdk	All	All	All	All

cpe:2.3:a:opensynergy:blue_sdk:*****:

cpe:2.3:a:opensynergy:blue_sdk:*****:

cpe:2.3:a:opensynergy:blue_sdk:*****:

No vendor comments have been submitted for this CVE

← 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](#)