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

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 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	Tags	Link
BlueSDK-advisory2018003 - OpenSynergy	Vendor Advisory www.opensynergy.com text/x-php	CONFIRM www.opensynergy.com/news/security/bluesdk-advisory2018003/
	Exploit Third Party Advisory www.cymotive.com application/pdf	MISC www.cymotive.com/wp-content/uploads/2019/03/Hell2CAP-0day.pdf

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→