



CVE-2020-5523

Published on: 01/28/2020 12:00:00 AM UTC

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

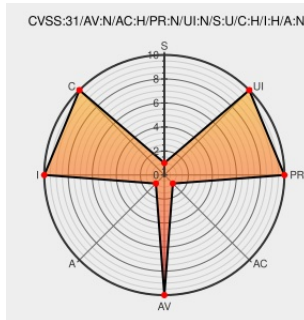
CVE-2020-5523

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [77 Bank](#) from [77bank](#) contain the following vulnerability:

Android App 'MyPallete' and some of the Android banking applications based on 'MyPallete' do not verify X.509 certificates from servers, and also do not properly validate certificates with host-mismatch, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

CVE-2020-5523 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [NTT Data Corporation](#) - 'MyPallete' and some of the Android banking applications that use 'MyPallete' version **MyPallete** all versions, **AshikagaBankingAppli** ver1.0.4 and earlier, **SENSHUIKEDABANKBankingAppli** ver3.0.4 and earlier, **ShikokuBankingAppli** ver2.0.1 and earlier, **TohokuBankingAppli** ver1.0.1 and earlier, **NaganoBankingAppli** ver1.0.1 and earlier, **77BankingAppli** ver2.0.1 and earlier, **HokkaidoBankingAppli** ver3.0.1 and earlier, and **HokurikuBankingAppli** ver2.0.1 and earlier

CVSS3 Score: **7.4 - HIGH**

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

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

Description	Tags	Link
	Third Party Advisory www.sihd-bk.jp application/pdf	 MISC www.sihd-bk.jp/common_v2/pdf/20200127.pdf
	Third Party Advisory www.77bank.co.jp application/pdf	 MISC www.77bank.co.jp/pdf/oshirase/20012801_appvulnerability.pdf
【どこでもバンク】あなたの新しいネットバンキング HOME	Third Party Advisory www.dokodemobank.ne.jp text/html	 MISC www.dokodemobank.ne.jp/info_20200128_bankingapp.html
とうぎんアプリにおけるSSL通信時の複数の脆弱性に関するお知らせ 東北銀行	Third Party Advisory www.tohoku-bank.co.jp text/html	 MISC www.tohoku-bank.co.jp/news/topics/200128_applissl.html
	Third Party Advisory www.ashikagabank.co.jp application/pdf	 MISC www.ashikagabank.co.jp/appbanking/pdf/oshirase.pdf
JVN#28845872: Android App "MyPallete" vulnerable to improper server certificate verification	Third Party Advisory jvn.jp text/xml	 MISC jvn.jp/en/jp/JVN28845872/index.html
ながぎんアプリにおけるSSL通信時の複数の脆弱性に関するお知らせ - 長野銀行	Third Party Advisory www.naganobank.co.jp text/xml	 MISC www.naganobank.co.jp/soshiki/2/app-ssl.html
『北陸銀行ポータルアプリ』におけるSSL通信時の脆弱性の修正に関するお知らせ お知らせ 北陸銀行	Third Party Advisory www.hokugin.co.jp text/html	 MISC www.hokugin.co.jp/info/archives/personal/2020/1913.html
	Third Party Advisory www.hokkaidobank.co.jp application/pdf	 MISC www.hokkaidobank.co.jp/common/dat/2020/0120/15795047141946146699.pdf
四国銀行アプリにおけるSSL通信時の複数の脆弱性に関するお知らせ 四国銀行	Third Party Advisory www.shikokubank.co.jp text/html	 MISC www.shikokubank.co.jp/info/apps20200128.html

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	77bank	77 Bank	All	All	All	All
Application	Ashikagabank	Ashigin	All	All	All	All
Application	Hokkaidobank	Dogin	All	All	All	All
Application	Hokugin	Hokuriku Bank Portal	All	All	All	All

Application	Naganobank	Nagagin	All	All	All	All
Application	Nttdata	Mypallete	-	All	All	All
Application	Nttdata	Mypallete	-	All	All	All
Application	Shikokubank	Shikoku Bank	All	All	All	All
Application	Sihd-bk	Ikedasenshubank	All	All	All	All
Application	Tohoku-bank	Tougin	All	All	All	All
cpe:2.3:a:77bank:77_bank:*:*:*:*:android:*:*:						
cpe:2.3:a:ashikagabank:ashigin:*:*:*:*:android:*:*:						
cpe:2.3:a:hokkaidobank:dogin:*:*:*:*:android:*:*:						
cpe:2.3:a:hokugin:hokuriku_bank_portal:*:*:*:*:android:*:*:						
cpe:2.3:a:naganobank:nagagin:*:*:*:*:android:*:*:						
cpe:2.3:a:nttdata:mypallete:-:*:*:*:*:android:*:*:						
cpe:2.3:a:nttdata:mypallete:-:*:*:*:*:android:*:*:						
cpe:2.3:a:shikokubank:shikoku_bank:*:*:*:*:android:*:*:						
cpe:2.3:a:sihd-bk:ikedasenshubank:*:*:*:*:android:*:*:						
cpe:2.3:a:tohoku-bank:tougin:*:*:*:*:android:*:*:						

© CVE.report 2023 |

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](#).