


Prüfbericht-Nr.: Test Report No.:	60364256 001	Auftrags-Nr.: Order No.:	168261459	Seite 1 von 8 Page 1 of 8
Kunden-Referenz-Nr.: Client Reference No.:	2127669	Auftragsdatum: Order date:	20.04.2020	
Auftraggeber: Client:	Xiaomi Communications Co., Ltd.			
Prüfgegenstand: Test item:	MIUI 12.0.1.0			
Bezeichnung / Typ-Nr.: Identification / Type No.:	Customized Android System (Software)			
Auftrags-Inhalt: Order content:	Privacy Protection Features			
Prüfgrundlage: Test specification:	安卓系统增强隐私保护测试 Enhanced Privacy Protection Testing Requirement for Android System			
Wareneingangsdatum: Date of receipt:	07.04.2020	 <p>已经是最新版本 MIUI V12.0.1.0 稳定版</p>		
Prüfmuster-Nr.: Test sample No.:	-			
Prüfzeitraum: Testing period:	07.04.2020 – 21.04.2020			
Ort der Prüfung: Place of testing:	TUV Rheinland Shenzhen			
Prüflaboratorium: Testing laboratory:	TUV Rheinland Shenzhen			
Prüfergebnis*: Test result*:	Pass			
geprüft von / tested by:		kontrolliert von / reviewed by:		
20.04.2020 Guangyi Wu / Test Engineer 		20.04.2020 Sven Olaf-Steinke / Reviewer 		
Datum Date	Name / Stellung Name / Position	Unterschrift Signature	Datum Date	Name / Stellung Name / Position
Datum Date	Name / Stellung Name / Position	Unterschrift Signature	Datum Date	Name / Stellung Name / Position
Sonstiges / Other: According to the test result of privacy protection features, TÜV Rheinland has reached a conclusion that MIUI is providing users with higher disposal rights, convenience and guidance regarding privacy. We conclude that MIUI has reached adequate privacy protection level according to the requirement. Test is based on MIUI 11 20.3.27 confidential version, the features are identical with MIUI 12.0.1.0.				
Zustand des Prüfgegenstandes bei Anlieferung: Condition of the test item at delivery:		Prüfmuster vollständig und unbeschädigt Test item complete and undamaged		
* Legende: 1 = sehr gut 2 = gut 3 = befriedigend 4 = ausreichend 5 = mangelhaft P(ass) = entspricht o.g. Prüfgrundlage(n) F(ail) = entspricht nicht o.g. Prüfgrundlage(n) N/A = nicht anwendbar N/T = nicht getestet Legend: 1 = very good 2 = good 3 = satisfactory 4 = sufficient 5 = poor P(ass) = passed a.m. test specification(s) F(ail) = failed a.m. test specification(s) N/A = not applicable N/T = not tested				
Dieser Prüfbericht bezieht sich nur auf das o.g. Prüfmuster und darf ohne Genehmigung der Prüfstelle nicht auszugsweise vervielfältigt werden. Dieser Bericht berechtigt nicht zur Verwendung eines Prüfzeichens. This test report only relates to the a. m. test sample. Without permission of the test center this test report is not permitted to be duplicated in extracts. This test report does not entitle to carry any test mark.				

V04

Prüfbericht-Nr.: 60364256 001
Test Report No.:

Seite 2 von 8
Page 2 of 8

Liste der verwendeten Prüfmittel
List of used test equipment

Prüfmittel <i>Test equipment</i>		Prüfmittel-Nr. / ID-Nr. <i>Equipment No. / ID-No.</i>	Nächste Kalibrierung <i>Next calibration</i>
-			
1	Produktdetails <i>Product details</i>	MIUI 12.0.1.0. Customized Android System(Software)	
2	Maße / Gewicht <i>Dimensions / Weight</i>	-	
3	Bedienelemente <i>Operating elements</i>	-	
4	Ausstattung / Zubehör <i>Equipment / Accessories</i>	-	
5	Verwendete Materialien <i>Used materials</i>	-	
6	Sonstiges <i>Other</i>	-	



已经是最新版本
MIUI V12.0.1.0 | 稳定版

Prüfbericht-Nr.: 60364256 001 <i>Test Report No.:</i>	Seite 4 von 8 Page 4 of 8
---	------------------------------

Absatz		Messergebnisse - Bemerkungen	Bewertung
Clause	Anforderungen - Prüfungen / Requirements - Tests	Measuring results - Remarks	Evaluation

	This testing requirement is aiming at providing uses with deeper understanding of the Android system, more convenience in controlling their privacy and higher disposal rights of private information.		
1	Permission Managment		
1.1	General Permission Management		
	a) User shall provide consent when an application is applying for permissions for the first time	Consent can be provided when and application is used for the first time.	P
	b) Applying for permission can only appear when the application is running, the application should be a popup window and ask for user consent	Customized pop window with the purpose of said request.	P
	c) Consent can be withdrawn, user can withdraw permission in a separate interface, change them from allow to prohibit or inquire. After permission is withdrawn, sub-group of under the permission group will all be withdrawn	Permission Access Location	P
		Permission Record Audio	P
	d) Sensitive permission group can be set to one time permission or permission when running. If permission is set to permission when running, then the entire permission group can't be used by the application after exit the application, if permission is set to one time permission, then the entire permission group can't be used after this exist.	Permission Phone state	P
		Permission Access location	P
		Permission Record Audio	P
		Permission Pictures and video	P
		Permission Read sensor data	P
		Permission Read/Write contact	P
		Permission Read/Write calendar	P
		Permission Read/Write Phone log	P
		Permission Read/Send Text Messages	P
1.2	Enhanced Permission Management		P
	a) When pre-installed applications and non pre-installed applications ask for permissions of	Permission Take Pictures and Video	P

Prüfbericht-Nr.: 60364256 001 Test Report No.:			Seite 5 von 8 Page 5 of 8
Absatz		Messergebnisse - Bemerkungen	Bewertung
Clause	Anforderungen - Prüfungen / Requirements - Tests	Measuring results - Remarks	Evaluation
	recording audio, photographing and recording video, and reading location information in the sensitive permission group, developers need to be based on clear, clear and reasonable purposes. When non pre-installed applications are submitted to the platform for distribution, developers need to provide clear, clear and reasonable purpose description for the call of these three permissions	Permission Access Location	P
		Permission Record Audio	P
	b) When the pre-installed application and non pre-installed application still use the sensitive permission group permission after entering the backstage, the system will automatically discover and give the user obvious reminders and identifications, and at the same time give the user quick access to set the permission (set to allow, inquire and prohibit only when the application is running).	Provide significant reminder for sensitive permission group, user can have quick access to set permission.	P
	c) When the pre-installed application and non pre-installed application call to read the clipboard permission limit, the system will automatically discover and give the user obvious reminders and marks, and at the same time give the user shortcut to set the permission (set to allow, inquire and prohibit only when the application is in use)	Clipboard permission can't be read or write when the application is running backstage.	P
2	Enhanced Privacy Protection Features		
2.1	Management of Unique Identification Code Android mobile phone system should generates an anonymous device identifier (OAID) for users, which can be manually reset by users, reset when restoring factory settings, reset by device manufacturers, and reset when installing new ROM, the scenarios of pre-installed application, non pre-installed application, user installed application using IMEI / IMSI / SN (ICCID) and other unique identification codes are all replaced with using anonymous device identifier (OAID). In order to prevent pre-installed applications and non pre-installed applications from accurately identify users in scenarios like personalized advertisement, targeted advertising.	OAID is in place to prevent IMEI/IMSI/SN overuse in targeted advertising. OAID can be restored by the user.	P
2.2	Privacy Protection Process		P

Prüfbericht-Nr.: 60364256 001 Test Report No.:			Seite 6 von 8 Page 6 of 8
Absatz		Messergebnisse - Bemerkungen	Bewertung
Clause	Anforderungen - Prüfungen / Requirements - Tests	Measuring results - Remarks	Evaluation
	Android platform provider should implement an appropriate privacy protection process to monitor the usage of non pre-installed applications. The goal is to monitor and protect the user, in the meantime manage the developers		
	a) User privacy protection User can provide feedback regarding the privacy protection of non pre-installed application. Platform should provide user with clear support and guidance on user interface and user experience, so that user can easily comprehend the content of the feedback, what response and outcome they can expect. User can receive response of their feedback in a proper timeframe. Suggested form of the response is system notice.	MIUI interface provided feature guidance and FAQ to support and guide user implementing the privacy protection features. MIUI interface provide privacy related entrance for feedback.	P
	b) Developer Privacy Protection When the platform discovered non-compliance items of non pre-installed applications uploaded by developer, proper notice should be sent to the developer advising modification.	Refer to clause 3.2. Found non-compliance items will be communicated with developers, but no mandatory action from MIUI is required	P
2.3	Special Privacy Protection Features The platform should provide special privacy protection features, protecting user privacy in special scenarios.		P
	a) Provide users with enhanced desensitization function. This kind of desensitization function can be activated in the situation that sensitive information may be leaked or disclosed, and the user can choose whether to enable it or not.	Sharing via photo gallery	P
		Multiple pics sharing via photo gallery	P
		Photo sharing via non pre-installed application	P
		Non-photo files sharing	P
	b) The system provides a function entrance to allow users to manage and modify the application's permission status, self-starting and pushing notifications.	MIUI provided entrance to users to manage and modify applications. Refer to 2.3 clause c.	P
	c) The system provides a function entrance, which allows users to see the application self-starting, chain starting, using sensitive permission group, high-risk behaviour and malicious behaviour in the	Application behaviour record	P
		Highlight, classification, weekly report, search function in application behaviour	P

Prüfbericht-Nr.: 60364256 001 Test Report No.:			Seite 7 von 8 Page 7 of 8
Absatz		Messergebnisse - Bemerkungen	Bewertung
Clause	Anforderungen - Prüfungen / Requirements - Tests	Measuring results - Remarks	Evaluation
	system for a period of time. Based on this entrance, users provide feedback on the application's self-starting, chain starting, using sensitive permission group call, high-risk behaviour and malicious behaviour to the platform.	record	
		Access location record	P
		Read/write text messages record	P
		Read/write clipboard record	P
		Read/write phone state record	P
		Self-starting record	P
		Chain-starting record	P
		Read/write storage record	P
		Camera usage record	P
		Phone call usage record	P
		Quick entrance to managing and modification of the application	P
3	Detection and interception of malicious and high risks behaviours		
3.1	Dangerous Permissions Detection and Interception If the application (pre-installed application, user installed application) invokes the device management application, displays on the upper layer of other applications, modifies system settings, automatically adjusts notifications, informs the right to use, installs the permissions of unknown applications, the system will automatically discover and intercept, after intercepting, it will give users obvious reminders and notification, and provide quick access for setting.	Refer to the application test report and results of 2.3	P
3.2	Application High Risk and Malicious Behaviours Detection and Interception The platform can detect applications (pre-installed applications, non pre-installed applications, user installed applications) dynamically and statically to find high-risk behaviours and malicious behaviours, and	Vulnerabilities detection like shell command, su root	P

Prüfbericht-Nr.: 60364256 001
Test Report No.:

Seite 8 von 8
Page 8 of 8

Absatz		Messergebnisse - Bemerkungen	Bewertung
Clause	Anforderungen - Prüfungen / Requirements - Tests	Measuring results - Remarks	Evaluation

	<p>provide users with enhanced privacy risk reminders.</p> <p>High risk and malicious behaviour refers to stealing user's privacy, excessive access, excessive use of permission, excessive collection of personal information, excessive use of personal information, as well as remote control, system damage, risk propagation, service overcharge, forced promotion, technology abuse and other behaviours of Android mobile terminal under the condition of user's unauthorized and unknown situation or skipping Android system application program interface.</p> <p>For pre-installed applications, non pre-installed applications and user installed applications, they can be detected in local, background or other environments.</p> <p>For the application installed by users themselves, it can provide protection for users through local detection and sensitive behaviour prompt and interception.</p> <p>The platform needs to avoid the collection and upload of user's personal information during the detection of application behaviour. If the user's personal data is necessary, the user's authorization is required. At the same time, the detection behaviour that needs the user's personal data support needs to be turned off by default and can only be turned on under the user's authorization.</p>	Excessive access application detection	P
		Excessive use of permission	P
		Potential user privacy stealing	P

Supporting documentation:

Application test report 1. pdf

Application test report 2. pdf

App store feedback reaction process. msg

OAID declaration. pdf

Permission declaration. pdf