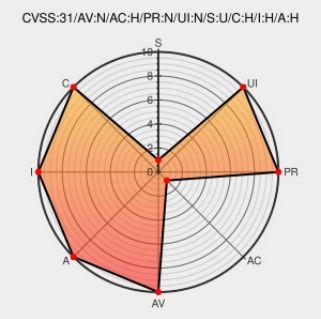
CVE-2019-15389

Published on: 11/14/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

CVE-2019-15389

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Haier A6 from Haier A6 Project contain the following vulnerability:

The Haier A6 Android device with a build fingerprint of Haier/A6/A6:8.1.0/O11019/1534219877:userdebug/release-keys contains a pre-installed platform app with a package name of com.lovelyfont.defcontainer (versionCode=7, versionName=7.1.13). This app contains an exported service named com.lovelyfont.manager.FontCoverService that allows any app co-located on the device to supply arbitrary commands to be executed as the system user. This app cannot be disabled by the user and the attack can be performed by a zero-permission app. In addition to the local attack surface, its accompanying app with a package name of com.ekesoo.lovelyhifonts makes network requests using HTTP and an attacker can perform a Man-in-the-Middle (MITM) attack on the connection to inject a command in a network response that will be executed as the system user by the com.lovelyfont.defcontainer app. Executing commands as the system user can allow a third-party app to video record the user's screen, factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the Graphical User Interface (GUI), and obtains the user's text messages, and more. Executing commands as the system user can allow a third-party app to factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the GUI, change the default Input Method Editor (IME) (e.g., keyboard) with one contained within the attacking app that contains keylogging functionality, and obtains the user's text messages, and more.

CVE-2019-15389 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

UNCHANGED HIGH HIGH HIGH

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Kryptowire Provides Details on Android Firmware Vulnerabilities - November 2019 - Kryptowire	Third Party Advisory www.kryptowire.com text/html	MISC www.kryptowire.com/android-firmware-2019/

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
Hardware	Haier A6 Project	Haier A6	-	All	All	All
Hardware	Haier A6 Project	Haier A6	-	All	All	All
Operating System	Haier A6 Project	Haier A6 Firmware	-	All	All	All
Operating System	Haier A6 Project	Haier A6 Firmware	-	All	All	All

cpe:2.3:h:haier_a6_project:haier_a6:-:*:*:*:*:*:*:*:

cpe:2.3:h:haier_a6_project:haier_a6:-:*:*:*:*:*:*:*:

cpe:2.3:o:haier_a6_project:haier_a6_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:haier_a6_project:haier_a6_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report