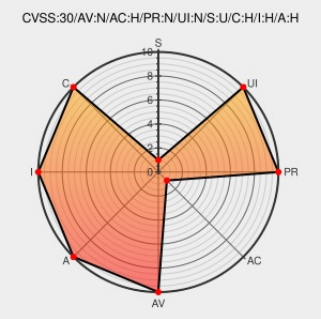
CVE-2018-11518

Published on: 05/30/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:17 PM UTC

CVE-2018-11518

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



Certain versions of Legacy Ivr from Hcltech contain the following vulnerability:

A vulnerability allows a phreaking attack on HCL legacy IVR systems that do not use VoIP. These IVR systems rely on various frequencies of audio signals; based on the frequency, certain commands and functions are processed. Since these frequencies are accepted within a phone call, an attacker can record these frequencies and use them for service activations. This is a request-forgery issue when the required series of DTMF signals for a service activation is predictable (e.g., the IVR system does not speak a nonce to the caller). In this case, the IVR system accepts an activation request from a less-secure channel (any loudspeaker in the caller's physical environment) without verifying that the request was intended (it matches a nonce sent over a more-secure channel to the caller's earpiece).

CVE-2018-11518 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: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Dhiraj 的 Twitter: “The IVR nowadays includes multiple functionalities like recharges and subscriptions for services which can also be done even with modern Telecom operators. #DiggingOldSys… https://t.co/QBdbZUiEli”	Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/mishradhiraj_/status/1001664440759091207
A Virgil's Guide to Pentest: 0day - Legacy IVR - Let's Phreak	Third Party Advisory virgil-cj.blogspot.com text/html	MISC virgil-cj.blogspot.com/2018/05/0day-legacy-ivr-lets-phreak.html
Abusing IVR Systems - Legacy Telecom [CVE-2018-11518] ~ inputzero	Third Party Advisory datarift.blogspot.com text/html	MISC datarift.blogspot.com/2018/05/CVE-2018-11518-abusing-ivr-systems.html
Dhiraj op Twitter: "Yes there is no boundry crossing here and it does follow the flow but the flow is controlled by someone else not the user who has initiated the call. Select 1 for English is just an example to show we can control other users flow without their consent. 1/n… https://t.co/rTME60EolO"	Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/mishradhiraj_/status/1001664204485652482

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Hcltech	Legacy Ivr	-	All	All	All
Hardware	Hcltech	Legacy Ivr	-	All	All	All
Operating System	Hcltech	Legacy Ivr Firmware	-	All	All	All
Operating System	Hcltech	Legacy Ivr Firmware	-	All	All	All

cpe:2.3:h:hcltech:legacy_ivr:-:*:*:*:*:*:*:*:

cpe:2.3:h:hcltech:legacy_ivr:-:*:*:*:*:*:*:*:

cpe:2.3:o:hcltech:legacy_ivr_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:hcltech:legacy_ivr_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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