



CVE-2019-1010200

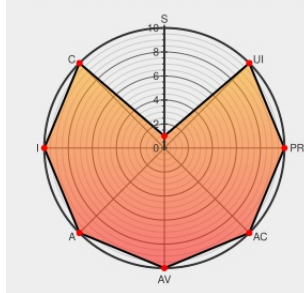
Published on: 07/23/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:57 PM UTC

CVE-2019-1010200

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Voice Builder](#) from [Google](#) contain the following vulnerability:

Voice Builder Prior to commit

c145d4604df67e6fc625992412eef0bf9a85e26b and

f6660e6d8f0d1d931359d591dbdec580fef36d36 is affected by: CWE-78: Improper Neutralization of Special Elements used in an OS

Command ('OS Command Injection'). The impact is: Remote code

execution with the same privileges as the servers. The component is: Two web servers in the projects expose three vulnerable endpoints that can be accessed remotely. The endpoints are defined at: - /tts: https://github.com/google/voice-builder/blob/3a449a3e8d5100ff323161c89b897f6d5ccdb6f9/merlin_model_server/api.js#L34 -

/alignment: https://github.com/google/voice-builder/blob/3a449a3e8d5100ff323161c89b897f6d5ccdb6f9/festival_model_server/api.js#L28 -

/tts: https://github.com/google/voice-builder/blob/3a449a3e8d5100ff323161c89b897f6d5ccdb6f9/festival_model_server/api.js#L65.

The attack vector is: Attacker sends a GET request to the vulnerable endpoint with a specially formatted query parameter. The fixed version is: After commit

f6660e6d8f0d1d931359d591dbdec580fef36d36.

CVE-2019-1010200 has been assigned by [GSD](#) cve-assign@distributedweaknessfiling.org to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [GSD](#) **Voice Builder - Voice Builder** version **Prior to commit c145d4604df67e6fc625992412eef0bf9a85e26b and f6660e6d8f0d1d931359d591dbdec580fef36d36 [fixed: After commit f6660e6d8f0d1d931359d591dbdec580fef36d36]**

CVSS3 Score: **9.8 - CRITICAL**

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

UNCHANGED

high

high

high

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Added function to replace characters with spaces and use it to sanitiz... · google/voice-builder@f6660e6 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/google/voice-builder/commit/f6660e6d8f0d1d931359d591dbdec580fef36d36
Added function to replace characters with space and use it to sanitiz... · google/voice-builder@c145d46 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/google/voice-builder/commit/c145d4604df67e6fc625992412eef0bf9a85e26b

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	Google	Voice Builder	-	All	All	All
Application	Google	Voice Builder	-	All	All	All

cpe:2.3:a:google:voice_builder:-:*:*:*:*:*:

cpe:2.3:a:google:voice_builder:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)