Re: [scr966035] your CVE ID requests

cve-request@mitre.org <cve-request@mitre.org>
周五 2022/7/15 13:24
收件人:
抄送:cve-request@mitre.org <cve-request@mitre.org>

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

> [Suggested description]
> An uncontrolled memory allocation issue was discovered in in the
> jerry_port_read_source function in the default-module.c file of
> Jerryscript 2.3.0, which can allow an attacker to perform a denial of
> service (DOS) via configuring an extra large javascript file or
> directory as an input file.
>
> --
>
> [VulnerabilityType Other]
> Uncontrolled memory allocation
>
> --
>
> [Vendor of Product]
> jerryscript
>
> --
>
> [Affected Product Code Base]
> jerryscript - 2.3.0
>
> --
>
> [Attack Type]
> Local
>
> --
>
> [Impact Denial of Service]
> true
>
> --
>
> [Attack Vectors]
> To exploit the vulnerability, an attacker can give an extra-large javascript file or a directory as an input file.
>
> --
>
> [Reference]
> https://github.com/jerryscript-project/jerryscript/issues/4251
> https://cwe.mitre.org/data/definitions/789.html
>

> --
>
> [Has vendor confirmed or acknowledged the vulnerability?]
> true
>
> --
>
> [Discoverer]
> discovered by a fuzzing tool developed by Lily Baihe Jiang

Use CVE-2020-26690.

> [Suggested description]
> Jerryscript v2.4.0 was discovered to contain a stack buffer overflow
> via the function jerryx_print_unhandled_exception in /util/print.c.
>
> --
>
> [Vulnerability Type]
> Buffer Overflow
>
> --
>
> [Vendor of Product]
> jerryscript
>
> --
>
> [Affected Product Code Base]
> jerryscript - 2.4.0
>
> --
>
> [Attack Type]
> Local
>
> --
>
> [Impact Information Disclosure]
> true
>
> --
>
> [Attack Vectors]
> The jerryscript engine will be attacked by executing a crafted javascript input.
>
> --
>
> [Reference]
> https://github.com/jerryscript-project/jerryscript/issues/5008
>
> --

>
> [Has vendor confirmed or acknowledged the vulnerability?]
> true
>
> --
>
> [Discoverer]
>

Use CVE-2022-32117.

- --
CVE Assignment Team
M/S M300, 202 Burlington Road, Bedford, MA 01730 USA
 [A PGP key is available for encrypted communications at
   https://cve.mitre.org/cve/request_id.html]
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQIcBAEBCAAGBQJi0Pm7AAoJENiPHH3233OGW+wP/RmsyYaZGevWG+rntrZNqwgS
k6yiOx/GP7lOAETClAk3sGP3mmcIbEeQnPC+QdvBfALLR5/acjBTaaXGUWEGzhKb
dFOmo6d8SmuDkKonIhjvikIM2gGmfrsF4OFijDVI8iHOa/FF4iW4dmb4OHEvnsnJ
ID6RwlSqOvup0pEHavkFoupKdeiS6/QYzqC86mh4D/yQsVPH+ymK3yC2V4UkhYI3
zV0kg2zOQ8tWkjTSiMeOpwHfMWfuA5N6NWF1zk4ks2U8Ccp+2r6Rpa4Mc6j9z+/s
2LZPuYa/wpU8LP6ooHB+Q1hcSh5OZ0yjNF90nAIsDrd7o07hzZoNm66eT3Jf47w3
BA5fo+q/1kIJrtRfaivgpk9C0RGATN6MVsfJrj9lH9nDwicy9f1zx6BrXrODS4Mn
uRIuloRa3Ejd7MIei5FHYbs8muzdoSkKvCP6UfQObv3KRBN9FyglYHeviFtKUIa4
dIkWZcuaKuF3O3h1QjiENi8fWVpgVW79sRqJTGZJsV9i15x07caSZBNcTVpQvmIp
Q9g3ZlA5WB2umGjv/2zJ7BV4X7FLXQQCHMmFHiPbGIlN5uMgvd02rkvWK140SOE3
16YIRDwbFmzN/D4VK++ZLXek6uWkojB+/NdtBx6amTgM9I0H0soHEjR/1DubjqVW
p0JU4YMGFiNlrYVo/DEg
=yGA2
-----END PGP SIGNATURE-----