



CVE-2019-5458

Published on: 07/30/2019 12:00:00 AM UTC

Last Modified on: 01/31/2023 09:17:00 PM UTC

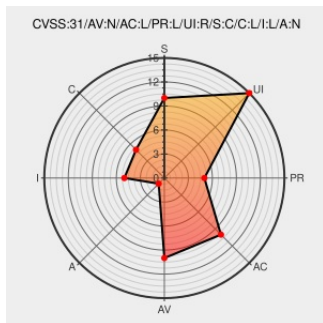
CVE-2019-5458

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Http-file-server](#) from [Http-file-server Project](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in http-file-server (all versions) allows an attacker with access to the server file system to execute arbitrary JavaScript code in victim's browser.

CVE-2019-5458 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [h1](#) **http-file-server** - **http-file-server** version **Not Fixed**

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
HackerOne	Exploit Third Party Advisory hackerone.com	h1 MISC hackerone.com/reports/570563

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	Http-file-server Project	Http-file-server	0.1.0	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.0	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.1	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.2	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.3	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.4	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.5	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.6	All	All	All
Application	Http-file-server Project	Http-file-server	0.1.0	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.0	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.1	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.2	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.3	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.4	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.5	All	All	All
Application	Http-file-server Project	Http-file-server	0.2.6	All	All	All

```
cpe:2.3:a:http-file-server_project:http-file-server:0.1.0:*:*:*:*:node.js:*:*
```

```
cpe:2.3:a:http-file-server_project:http-file-server:0.2.0:*:*:*:node.js:*:*
```

```
cpe:2.3:a:http-file-server_project:http-file-server:0.2.1:*:*:*:*:node.js:*:*
```

```
cpe:2.3:a:http-file-server_project:http-file-server:0.2.2:*:*:*:*:node.js:*:*
```

```
cpe:2.3:a:http-file-server_project:http-file-server:0.2.3:*:*:*:*:node.js:*:*
```

```
cpe:2.3:a:http-file-server_project:http-file-server:0.2.4:*:*:*:*:node.js:*:*
```

```
cpe:2.3:a:http-file-server project:http-file-server:0.2.5:*:*:*:node.js:*:
```

```
cpe:2.3:a:http-file-server project:http-file-server:0.2.6:*:*:*:*:node.js:*:*
```

```

--no-D 0: disable file server --no-include 0: disable file server
--no-D 1 0:***.***.***.***:***.***.***.***:***.***.***.***:***.***.***.***

```

cpe:2.3:a:ntp-mie-server_project:ntp-mie-server:0.1.0:*:*:*:*:node.js:*:*:
cpe:2.3:a:http-file-server_project:http-file-server:0.2.0:*:*:*:*:node.js:*:*:
cpe:2.3:a:http-file-server_project:http-file-server:0.2.1:*:*:*:*:node.js:*:*:
cpe:2.3:a:http-file-server_project:http-file-server:0.2.2:*:*:*:*:node.js:*:*:
cpe:2.3:a:http-file-server_project:http-file-server:0.2.3:*:*:*:*:node.js:*:*:
cpe:2.3:a:http-file-server_project:http-file-server:0.2.4:*:*:*:*:node.js:*:*:
cpe:2.3:a:http-file-server_project:http-file-server:0.2.5:*:*:*:*:node.js:*:*:
cpe:2.3:a:http-file-server_project:http-file-server:0.2.6:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)