



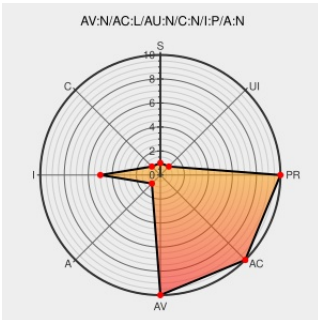
Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2068

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Freebsd](#) from [Freebsd](#) contain the following vulnerability:

FreeBSD 4.x through 4.11 and 5.x through 5.4 allows remote attackers to modify certain TCP options via a TCP packet with the SYN flag set for an already established session.

CVE-2005-2068 has been assigned by secteam@freebsd.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
	ftp.freebsd.org text/plain Inactive Link Not Archived	 FREEBSD FreeBSD-SA-05:15

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
Operating System	Freebsd	Freebsd	4.0	All	All	All
Operating System	Freebsd	Freebsd	4.1	All	All	All
Operating System	Freebsd	Freebsd	4.1.1	All	All	All
Operating System	Freebsd	Freebsd	4.10	All	All	All
Operating System	Freebsd	Freebsd	4.11	All	All	All
Operating System	Freebsd	Freebsd	4.2	All	All	All
Operating System	Freebsd	Freebsd	4.3	All	All	All
Operating System	Freebsd	Freebsd	4.4	All	All	All
Operating System	Freebsd	Freebsd	4.5	All	All	All
Operating System	Freebsd	Freebsd	4.6	All	All	All
Operating System	Freebsd	Freebsd	4.6.2	All	All	All
Operating System	Freebsd	Freebsd	4.7	All	All	All
Operating System	Freebsd	Freebsd	4.8	All	All	All
Operating System	Freebsd	Freebsd	4.9	All	All	All
Operating System	Freebsd	Freebsd	5.0	All	All	All
Operating System	Freebsd	Freebsd	5.1	All	All	All
Operating System	Freebsd	Freebsd	5.2	All	All	All
Operating System	Freebsd	Freebsd	5.2.1	All	All	All
Operating System	Freebsd	Freebsd	5.3	All	All	All
Operating System	Freebsd	Freebsd	5.4	All	All	All
Operating System	Freebsd	Freebsd	4.0	All	All	All
Operating System	Freebsd	Freebsd	4.1	All	All	All
Operating System	Freebsd	Freebsd	4.1.1	All	All	All

Operating System	Freebsd	Freebsd	4.0	All	All	All
Operating System	Freebsd	Freebsd	4.10	All	All	All
Operating System	Freebsd	Freebsd	4.11	All	All	All
Operating System	Freebsd	Freebsd	4.2	All	All	All
Operating System	Freebsd	Freebsd	4.3	All	All	All
Operating System	Freebsd	Freebsd	4.4	All	All	All
Operating System	Freebsd	Freebsd	4.5	All	All	All
Operating System	Freebsd	Freebsd	4.6	All	All	All
Operating System	Freebsd	Freebsd	4.6.2	All	All	All
Operating System	Freebsd	Freebsd	4.7	All	All	All
Operating System	Freebsd	Freebsd	4.8	All	All	All
Operating System	Freebsd	Freebsd	4.9	All	All	All
Operating System	Freebsd	Freebsd	5.0	All	All	All
Operating System	Freebsd	Freebsd	5.1	All	All	All
Operating System	Freebsd	Freebsd	5.2	All	All	All
Operating System	Freebsd	Freebsd	5.2.1	All	All	All
Operating System	Freebsd	Freebsd	5.3	All	All	All
Operating System	Freebsd	Freebsd	5.4	All	All	All
cpe:2.3:o:freebsd:freebsd:4.0:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:4.1:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:4.1.1:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:4.10:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:4.11:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:4.2:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:4.2.*:*:*:*:*:						

УРЕ.З.У.У.ИГЕУСУ.ИГЕУСУ.Т.У.

```
cpe:2.3:o:freebsd:freebsd:4.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.5:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.6:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.6.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.7:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.8:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.9:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:5.0:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:5.1:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:5.2:*:*:*:*:*.*
```

```
cpe:2.3:o:freebsd:freebsd:5.2.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:5.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:5.4:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.0:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.1:*.:*:*:*:*.*
```

```
cpe:2.3:o:freebsd:freebsd:4.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.10:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.11:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.2:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.3:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.4:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.5:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.6:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.6.2:*:*:*:*:*.*
```

```
cpe:2.3:o:freebsd:freebsd:4.7:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.8:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.9:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:5.0:*:*:*:*:*:*:
```

cpe:2.3:o:freebsd:freebsd:5.1:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:5.2:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:5.2.1:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:5.3:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:5.4:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →