



# CVE-2004-2679

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

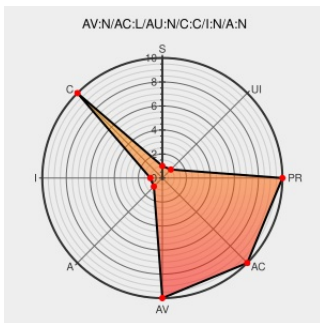
## CVE-2004-2679

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Firewall-1](#) from [Checkpoint](#) contain the following vulnerability:

Check Point Firewall-1 4.1 up to NG AI R55 allows remote attackers to obtain potentially sensitive information by sending an Internet Key Exchange (IKE) with a certain Vendor ID payload that causes Firewall-1 to return a response containing version and other information.

CVE-2004-2679 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access  
Vector

Access  
Complexity

Authentication

**NETWORK**

**LOW**

**NONE**

Confidentiality  
Impact

Integrity  
Impact

Availability  
Impact

**COMPLETE**

**NONE**

**NONE**

## CVE References

Description

Tags

Link

Check Point Firewall-1 Internet Key Exchange Information Disclosure Vulnerability

[cve.report \(archive\)](#)  
[text/html](#)

[🌐](#) [BID 10558](#)

NTA news

[www.nta-monitor.com](#)  
[text/html](#)

[🌐](#) [MISC www.nta-monitor.com/news/checkpoint2004/index.htm](#)

Neohapsis Archives - Full Disclosure List - #0477 - [Full-Disclosure] Checkpoint Firewall-1 IKE Vendor ID information leakage

[web.archive.org](#)  
[text/html](#)  
[Inactive Link](#) [Not Archived](#)

[🌐](#) [FULLDISC 20040616 Checkpoint Firewall-1 IKE Vendor ID information leakage](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)  
[text/html](#)

[🔗](#) [XF fw1-vendorid-info-disclosure\(16434\)](#)

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

This report does not endorse any commercial products that may be mentioned in these entries. Please address comments about any linked pages to [comment@cve.report](mailto: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 | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | All    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp1    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp2    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp3    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp4    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp5    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp6    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp7    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp8    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | All    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | sp1    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | sp2    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | sp3    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | sp4    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | sp5    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | sp5a   | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | sp6    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | r55     | All    | ng-ai   | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | All    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp1    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp2    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp3    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp4    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp5    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp6    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp7    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.0     | sp8    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | All    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | sp1    | All     | All      |
| Application | <a href="#">Checkpoint</a> | <a href="#">Firewall-1</a> | 4.1     | sp2    | All     | All      |



|                                                        |
|--------------------------------------------------------|
| cpe:2.3:a:checkpoint:firewall-1:4.0:sp5:*:*:*:*:*:     |
| cpe:2.3:a:checkpoint:firewall-1:4.0:sp6:*:*:*:*:*:     |
| cpe:2.3:a:checkpoint:firewall-1:4.0:sp7:*:*:*:*:*:     |
| cpe:2.3:a:checkpoint:firewall-1:4.0:sp8:*:*:*:*:*:     |
| cpe:2.3:a:checkpoint:firewall-1:4.1:*:*:*:*:*:         |
| cpe:2.3:a:checkpoint:firewall-1:4.1:sp1:*:*:*:*:*:     |
| cpe:2.3:a:checkpoint:firewall-1:4.1:sp2:*:*:*:*:*:     |
| cpe:2.3:a:checkpoint:firewall-1:4.1:sp3:*:*:*:*:*:     |
| cpe:2.3:a:checkpoint:firewall-1:4.1:sp4:*:*:*:*:*:     |
| cpe:2.3:a:checkpoint:firewall-1:4.1:sp5:*:*:*:*:*:     |
| cpe:2.3:a:checkpoint:firewall-1:4.1:sp5a:*:*:*:*:*:    |
| cpe:2.3:a:checkpoint:firewall-1:4.1:sp6:*:*:*:*:*:     |
| cpe:2.3:a:checkpoint:firewall-1:r55:*:ng-ai:*:*:*:*:*: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→