



CVE-2013-5635

Published on: 11/30/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:36 PM UTC

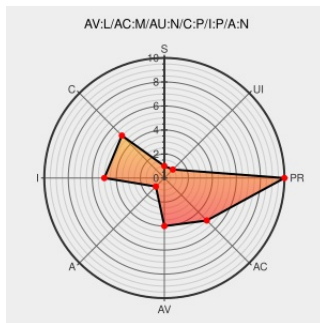
CVE-2013-5635

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Endpoint Security](#) from [Checkpoint](#) contain the following vulnerability:

Media Encryption EPM Explorer in Check Point Endpoint Security through E80.50 does not properly maintain the state of password failures, which makes it easier for physically proximate attackers to bypass the device-locking protection mechanism by entering password guesses within multiple Unlock.exe processes that are running

simultaneously.

CVE-2013-5635 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **3.3 - LOW**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

www.digitalsec.net
[text/plain](#)

[MISC](#)
www.digitalsec.net/stuff/exploit+advs/CheckPoint_EndPoint_EPM_Explorer.txt

Check Point response to Media Encryption EPM Explorer lockout bypass (CVE-2013-5635 and CVE-2013-5636)

[Patch](#)
supportcenter.checkpoint.com
[application/octet-stream](#)

[CONFIRM](#) supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk96589

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

cpe:2.3:a:checkpoint:endpoint_security:e80.50::-:vpn_blade:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)