



# Lock screen setting bypass in Firefox Focus for Android

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2025-1941
<b>State</b>	PUBLISHED
<b>Assigner</b>	mozilla
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-03-04 14:15:39 UTC
<b>Updated</b>	2026-04-13 15:16:53 UTC
<b>Description</b>	Under certain circumstances, a user opt-in setting that Focus should require authentication before use could have been be

## Risk And Classification

**Primary CVSS:** v3.1 9.1 CRITICAL from ADP

**CVSS:** [3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N](#)

**EPSS:** 0.000660000 probability, percentile 0.204910000 (date 2026-04-15)

**Problem Types:** CWE-284 | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.1	CRITICAL	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N</a>
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.1	CRITICAL	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N</a>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**High**

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mozilla	Firefox	unaffected 136 * rpm	Not specified

### References

Reference	Source	Link	Tags
bugzilla.mozilla.org/show_bug.cgi	security@mozilla.org	bugzilla.mozilla.org	Issue Tracking
www.mozilla.org/security/advisories/mfsa2025-14	security@mozilla.org	www.mozilla.org	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** Jurrie Overgoor (en)

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)