



# CVE-2021-22299

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-22299
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@huawei.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-06 02:15:00 UTC
<b>Updated</b>	2022-07-12 17:42:00 UTC
<b>Description</b>	There is a local privilege escalation vulnerability in some Huawei products. A local, authenticated attacker could craft specif

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Huawei</a>	<a href="#">Imaster Mae-m</a>	v100r020c10spc220	All	All	All
Application	<a href="#">Huawei</a>	<a href="#">Imaster Mae-m</a>	v100r020c10spc220	All	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.0	-	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.0	rc2.b050	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.0	spc100.b210	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	-	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	rc1.b060	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	rc2.b020	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	rc2.b030	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	rc2.b040	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	rc2.b050	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	rc2.b060	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	rc2.b070	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	rc2.b080	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	rc2.b090	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	spc100.b050	All	All
Application	<a href="#">Huawei</a>	<a href="#">Manageone</a>	6.5.1	spc101.b010	All	All

Application	Huawei	Manageone	6.5.1	spc101.b040	All	All
Application	Huawei	Manageone	6.5.1	spc200	All	All
Application	Huawei	Manageone	6.5.1	spc200.b010	All	All
Application	Huawei	Manageone	6.5.1	spc200.b030	All	All
Application	Huawei	Manageone	6.5.1	spc200.b040	All	All
Application	Huawei	Manageone	6.5.1	spc200.b050	All	All
Application	Huawei	Manageone	6.5.1	spc200.b060	All	All
Application	Huawei	Manageone	6.5.1	spc200.b070	All	All
Application	Huawei	Manageone	6.5.1.1	b010	All	All
Application	Huawei	Manageone	6.5.1.1	b020	All	All
Application	Huawei	Manageone	6.5.1.1	b030	All	All
Application	Huawei	Manageone	6.5.1.1	b040	All	All
Application	Huawei	Manageone	8.0.0	-	All	All
Application	Huawei	Manageone	8.0.0	lcnd81	All	All
Application	Huawei	Manageone	8.0.0	rc2	All	All
Application	Huawei	Manageone	8.0.0	rc3	All	All
Application	Huawei	Manageone	8.0.0	rc3.b041	All	All
Application	Huawei	Manageone	8.0.0	rc3.spc100	All	All
Application	Huawei	Manageone	8.0.0	spc100	All	All
Application	Huawei	Manageone	8.0.1	All	All	All
Application	Huawei	Manageone	6.5.0	-	All	All
Application	Huawei	Manageone	6.5.0	rc2.b050	All	All
Application	Huawei	Manageone	6.5.0	spc100.b210	All	All
Application	Huawei	Manageone	6.5.1	-	All	All
Application	Huawei	Manageone	6.5.1	rc1.b060	All	All
Application	Huawei	Manageone	6.5.1	rc2.b020	All	All
Application	Huawei	Manageone	6.5.1	rc2.b030	All	All
Application	Huawei	Manageone	6.5.1	rc2.b040	All	All
Application	Huawei	Manageone	6.5.1	rc2.b050	All	All
Application	Huawei	Manageone	6.5.1	rc2.b060	All	All
Application	Huawei	Manageone	6.5.1	rc2.b070	All	All
Application	Huawei	Manageone	6.5.1	rc2.b080	All	All
Application	Huawei	Manageone	6.5.1	rc2.b090	All	All
Application	Huawei	Manageone	6.5.1	spc100.b050	All	All
Application	Huawei	Manageone	6.5.1	spc101.b010	All	All

Application	Huawei	Manageone	6.5.1	spc101.b040	All	All
Application	Huawei	Manageone	6.5.1	spc200	All	All
Application	Huawei	Manageone	6.5.1	spc200.b010	All	All
Application	Huawei	Manageone	6.5.1	spc200.b030	All	All
Application	Huawei	Manageone	6.5.1	spc200.b040	All	All
Application	Huawei	Manageone	6.5.1	spc200.b050	All	All
Application	Huawei	Manageone	6.5.1	spc200.b060	All	All
Application	Huawei	Manageone	6.5.1	spc200.b070	All	All
Application	Huawei	Manageone	6.5.1.1	b010	All	All
Application	Huawei	Manageone	6.5.1.1	b020	All	All
Application	Huawei	Manageone	6.5.1.1	b030	All	All
Application	Huawei	Manageone	6.5.1.1	b040	All	All
Application	Huawei	Manageone	8.0.0	-	All	All
Application	Huawei	Manageone	8.0.0	lcnd81	All	All
Application	Huawei	Manageone	8.0.0	rc2	All	All
Application	Huawei	Manageone	8.0.0	rc3	All	All
Application	Huawei	Manageone	8.0.0	rc3.b041	All	All
Application	Huawei	Manageone	8.0.0	rc3.spc100	All	All
Application	Huawei	Manageone	8.0.0	spc100	All	All
Application	Huawei	Manageone	8.0.1	All	All	All
Application	Huawei	Network Functions Virtualization Fusionsphere	6.5.1	spc12	All	All
Application	Huawei	Network Functions Virtualization Fusionsphere	6.5.1	spc23	All	All
Application	Huawei	Network Functions Virtualization Fusionsphere	6.5.1	spc12	All	All
Application	Huawei	Network Functions Virtualization Fusionsphere	6.5.1	spc23	All	All
Hardware	Huawei	Smc2.0	-	All	All	All
Hardware	Huawei	Smc2.0	-	All	All	All
Hardware	Huawei	Smc2.0	-	All	All	All
Operating System	Huawei	Smc2.0 Firmware	v600r019c00	All	All	All
Operating System	Huawei	Smc2.0 Firmware	v600r019c10	All	All	All
Operating System	Huawei	Smc2.0 Firmware	v600r019c00	All	All	All
Operating System	Huawei	Smc2.0 Firmware	v600r019c10	All	All	All

## References

Reference	Source	Link	Tags
Security Advisory - Local Privilege Escalation Vulnerability in Some Huawei Products	CONFIRM	<a href="http://www.huawei.com">www.huawei.com</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)