



# CVE-2019-12762

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2019-12762  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2019-06-06 20:29:00 UTC   |
| <b>Updated</b>         | 2023-11-07 03:03:00 UTC   |
| <b>Description</b>     | Xiaomi Mi 5s Plus devices allow attackers to trigger touchscreen anomalies via a radio signal between 198 kHz and 203 kHz |

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                  | Product                                   | Version | Update | Edition | Language |
|------------------|-------------------------|---|---------|--------|---------|----------|
| Hardware         | <a href="#">Fujitsu</a> | <a href="#">Arrows Nx F005-f</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Fujitsu</a> | <a href="#">Arrows Nx F005-f</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Fujitsu</a> | <a href="#">Arrows Nx F005-f Firmware</a> | -       | All    | All     | All      |
| Operating System | <a href="#">Fujitsu</a> | <a href="#">Arrows Nx F005-f Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Fujitsu</a> | <a href="#">Arrows Nx F05-f</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Fujitsu</a> | <a href="#">Arrows Nx F05-f Firmware</a>  | -       | All    | All     | All      |
| Hardware         | <a href="#">Google</a>  | <a href="#">Nexus 7</a>                   | -       | All    | All     | All      |
| Hardware         | <a href="#">Google</a>  | <a href="#">Nexus 7</a>                   | -       | All    | All     | All      |
| Operating System | <a href="#">Google</a>  | <a href="#">Nexus 7 Firmware</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Google</a>  | <a href="#">Nexus 7 Firmware</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Google</a>  | <a href="#">Nexus 9</a>                   | -       | All    | All     | All      |
| Hardware         | <a href="#">Google</a>  | <a href="#">Nexus 9</a>                   | -       | All    | All     | All      |
| Operating System | <a href="#">Google</a>  | <a href="#">Nexus 9 Firmware</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Google</a>  | <a href="#">Nexus 9 Firmware</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Mi</a>      | <a href="#">Mi 5s Plus</a>                | -       | All    | All     | All      |
| Operating System | <a href="#">Mi</a>      | <a href="#">Mi 5s Plus Firmware</a>       | -       | All    | All     | All      |
| Hardware         | <a href="#">Samsung</a> | <a href="#">Galaxy S4</a>                 | -       | All    | All     | All      |

|                  |         |                            |   |     |     |     |
|------------------|---------|----------------------------|---|-----|-----|-----|
| Hardware         | Samsung | Galaxy S4                  | - | All | All | All |
| Operating System | Samsung | Galaxy S4 Firmware         | - | All | All | All |
| Operating System | Samsung | Galaxy S4 Firmware         | - | All | All | All |
| Hardware         | Samsung | Galaxy S6 Edge             | - | All | All | All |
| Hardware         | Samsung | Galaxy S6 Edge             | - | All | All | All |
| Operating System | Samsung | Galaxy S6 Edge Firmware    | - | All | All | All |
| Operating System | Samsung | Galaxy S6 Edge Firmware    | - | All | All | All |
| Hardware         | Sharp   | Aquos Zeta Sh-04f          | - | All | All | All |
| Hardware         | Sharp   | Aquos Zeta Sh-04f          | - | All | All | All |
| Operating System | Sharp   | Aquos Zeta Sh-04f Firmware | - | All | All | All |
| Operating System | Sharp   | Aquos Zeta Sh-04f Firmware | - | All | All | All |
| Hardware         | Sony    | Xperia Z4                  | - | All | All | All |
| Hardware         | Sony    | Xperia Z4                  | - | All | All | All |
| Operating System | Sony    | Xperia Z4 Firmware         | - | All | All | All |
| Operating System | Sony    | Xperia Z4 Firmware         | - | All | All | All |
| Hardware         | Xiaomi  | Mi 5s Plus                 | - | All | All | All |
| Hardware         | Xiaomi  | Mi 5s Plus                 | - | All | All | All |
| Operating System | Xiaomi  | Mi 5s Plus Firmware        | - | All | All | All |
| Operating System | Xiaomi  | Mi 5s Plus Firmware        | - | All | All | All |

## References

| Reference   | Source  | Link   | Tags                          |
|---|---------|--|-------------------------------|
| NFC Vulnerability May Promote Ghost Screen Taps                 | MISC    | <a href="http://hackercombat.com">hackercombat.com</a> | Third Party Advisory          |
| Ghost Touch on Xiaomi Mi5s Plus   by julio della flora   Medium |         | <a href="http://medium.com">medium.com</a>             |                               |
| Ghost Touch on Xiaomi Mi5s Plus   by julio della flora   Medium | MISC    | <a href="http://medium.com">medium.com</a>             | Exploit, Third Party Advisory |
| CVE Program record  | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>           | canonical                     |
| NVD vulnerability detail  | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>         | canonical, analysis           |

No vendor comments have been submitted for this CVE.

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

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](#)**