



CVE-2018-20523

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-20523 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-06-07 16:29:00 UTC |
| Updated | 2022-04-19 15:36:00 UTC |
| Description | Xiaomi Stock Browser 10.2.4.g on Xiaomi Redmi Note 5 Pro devices and other Redmi Android phones allows content provi |

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|-----------------------|---------|--------|---------|----------|
| Hardware | Mi | Redmi 4a | - | All | All | All |
| Hardware | Mi | Redmi 4a | - | All | All | All |
| Operating System | Mi | Redmi 4a Firmware | - | All | All | All |
| Operating System | Mi | Redmi 4a Firmware | - | All | All | All |
| Hardware | Mi | Redmi 5 Plus | - | All | All | All |
| Hardware | Mi | Redmi 5 Plus | - | All | All | All |
| Operating System | Mi | Redmi 5 Plus Firmware | - | All | All | All |
| Operating System | Mi | Redmi 5 Plus Firmware | - | All | All | All |
| Hardware | Mi | Redmi 6 | - | All | All | All |
| Hardware | Mi | Redmi 6 | - | All | All | All |
| Hardware | Mi | Redmi 6a | - | All | All | All |
| Hardware | Mi | Redmi 6a | - | All | All | All |
| Operating System | Mi | Redmi 6a Firmware | - | All | All | All |
| Operating System | Mi | Redmi 6a Firmware | - | All | All | All |
| Operating System | Mi | Redmi 6 Firmware | - | All | All | All |
| Operating System | Mi | Redmi 6 Firmware | - | All | All | All |
| Hardware | Mi | Redmi 7 | - | All | All | All |

| | | | | | | |
|------------------|----|------------------------------|---|-----|-----|-----|
| Hardware | Mi | Redmi 7 | - | All | All | All |
| Hardware | Mi | Redmi 7a | - | All | All | All |
| Hardware | Mi | Redmi 7a | - | All | All | All |
| Operating System | Mi | Redmi 7a Firmware | - | All | All | All |
| Operating System | Mi | Redmi 7a Firmware | - | All | All | All |
| Operating System | Mi | Redmi 7 Firmware | - | All | All | All |
| Operating System | Mi | Redmi 7 Firmware | - | All | All | All |
| Hardware | Mi | Redmi Go | - | All | All | All |
| Hardware | Mi | Redmi Go | - | All | All | All |
| Operating System | Mi | Redmi Go Firmware | - | All | All | All |
| Operating System | Mi | Redmi Go Firmware | - | All | All | All |
| Hardware | Mi | Redmi K20 | - | All | All | All |
| Hardware | Mi | Redmi K20 | - | All | All | All |
| Operating System | Mi | Redmi K20 Firmware | - | All | All | All |
| Operating System | Mi | Redmi K20 Firmware | - | All | All | All |
| Hardware | Mi | Redmi K20 Pro | - | All | All | All |
| Hardware | Mi | Redmi K20 Pro | - | All | All | All |
| Operating System | Mi | Redmi K20 Pro Firmware | - | All | All | All |
| Operating System | Mi | Redmi K20 Pro Firmware | - | All | All | All |
| Hardware | Mi | Redmi Note 4 | - | All | All | All |
| Hardware | Mi | Redmi Note 4 | - | All | All | All |
| Operating System | Mi | Redmi Note 4 Firmware | - | All | All | All |
| Operating System | Mi | Redmi Note 4 Firmware | - | All | All | All |
| Hardware | Mi | Redmi Note 5 | - | All | All | All |
| Hardware | Mi | Redmi Note 5 | - | All | All | All |
| Hardware | Mi | Redmi Note 5a Prime | - | All | All | All |
| Hardware | Mi | Redmi Note 5a Prime | - | All | All | All |
| Operating System | Mi | Redmi Note 5a Prime Firmware | - | All | All | All |
| Operating System | Mi | Redmi Note 5a Prime Firmware | - | All | All | All |
| Operating System | Mi | Redmi Note 5 Firmware | - | All | All | All |
| Operating System | Mi | Redmi Note 5 Firmware | - | All | All | All |
| Hardware | Mi | Redmi Note 5 Pro | - | All | All | All |
| Hardware | Mi | Redmi Note 5 Pro | - | All | All | All |
| Operating System | Mi | Redmi Note 5 Pro Firmware | - | All | All | All |
| Operating System | Mi | Redmi Note 5 Pro Firmware | - | All | All | All |

| | | | | | | |
|------------------|----|---------------------------|---------|-----|-----|-----|
| Hardware | Mi | Redmi Note 6 Pro | - | All | All | All |
| Hardware | Mi | Redmi Note 6 Pro | - | All | All | All |
| Operating System | Mi | Redmi Note 6 Pro Firmware | - | All | All | All |
| Operating System | Mi | Redmi Note 6 Pro Firmware | - | All | All | All |
| Hardware | Mi | Redmi Note 7 | - | All | All | All |
| Hardware | Mi | Redmi Note 7 | - | All | All | All |
| Hardware | Mi | Redmi Note 7s | - | All | All | All |
| Hardware | Mi | Redmi Note 7s | - | All | All | All |
| Operating System | Mi | Redmi Note 7s Firmware | - | All | All | All |
| Operating System | Mi | Redmi Note 7s Firmware | - | All | All | All |
| Operating System | Mi | Redmi Note 7 Firmware | - | All | All | All |
| Operating System | Mi | Redmi Note 7 Firmware | - | All | All | All |
| Hardware | Mi | Redmi S2 | - | All | All | All |
| Hardware | Mi | Redmi S2 | - | All | All | All |
| Operating System | Mi | Redmi S2 Firmware | - | All | All | All |
| Operating System | Mi | Redmi S2 Firmware | - | All | All | All |
| Hardware | Mi | Redmi Y3 | - | All | All | All |
| Hardware | Mi | Redmi Y3 | - | All | All | All |
| Operating System | Mi | Redmi Y3 Firmware | - | All | All | All |
| Operating System | Mi | Redmi Y3 Firmware | - | All | All | All |
| Application | Mi | Stock Browser | 10.2.4g | All | All | All |
| Application | Mi | Stock Browser | 10.2.4g | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|---|----------------------|
| 小米安全中心 | MISC | sec.xiaomi.com | Vendor Advisory |
| Xiaomi 10.2.4.g Information Disclosure ≈ Packet Storm | MISC | packetstormsecurity.com | |
| Content provider injection in Xiaomi stock browser – Vishwaraj Bhattraï | MISC | vishwarajbhattraï.wordpress.com | Exploit, Third Party |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

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](#).

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