APP-26 · Mobile Threat Catalogue

Archived: 2026-04-05 16:03:46 UTC

Mobile Threat Catalogue

Privilage Escalation via OS Vulnerability

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-26

Threat Description: Malicious applications that achieve privilege escalation in the context of the mobile OS, driver, peripheral firmware, or the kernel, may further achieve unauthorized access or modification of app, user, or system data, process memory, or execute other unauthorized actions on the device.

Threat Origin

Dissecting Android Malware: Characterization and Evolution [1]

Exploit Examples

CVE Examples

- CVE-2017-2398
- CVE-2017-2401
- CVE-2017-2440
- CVE-2017-2451
- CVE-2017-2456
- CVE-2017-2472
- CVE-2017-2473
- CVE-2017-2474
- CVE-2017-2478
- CVE-2017-2482
- CVE-2017-2483
- CVE-2017-2490
- CVE-2017-0593
- CVE-2017-0598
- CVE-2017-0601
- CVE-2016-7056
- CVE-2016-10274
- CVE-2016-10275

- CVE-2016-10276
- CVE-2016-9794
- CVE-2017-0331
- CVE-2017-0604
- CVE-2017-0605
- CVE-2016-10280
- CVE-2016-10281
- CVE-2016-10282
- CVE-2016-10283
- CVE-2016-10284
- CVE-2016-10285
- CVE-2016-10286
- CVE-2015-9004
- CVE-2016-10287
- CVE-2017-0606
- CVE-2016-5860
- CVE-2016-5867
- CVE-2017-0607
- CVE-2017-0608
- CVE-2017-0609
- CVE-2016-5859
- CVE-2017-0610
- CVE-2017-0611
- CVE-2016-5853
- CVE-2016-10288
- CVE-2016-10289
- CVE-2016-10290
- CVE-2017-0465
- CVE-2017-0612
- CVE-2017-0613
- CVE-2017-0614
- CVE-2017-0616
- CVE-2017-0618
- CVE-2017-0619
- CVE-2017-0620
- CVE-2016-5862
- CVE-2017-0621
- CVE-2016-5868
- CVE-2017-0622
- CVE-2017-0623
- CVE-2017-0624
- CVE-2017-0625

- CVE-2017-0626
- CVE-2017-0627
- CVE-2016-10293
- CVE-2016-10294
- CVE-2016-10295
- CVE-2016-10296
- CVE-2017-0628
- CVE-2017-0629
- CVE-2017-0630
- CVE-2016-5858
- CVE-2017-0631
- CVE-2016-5347
- CVE-2016-5854
- CVE-2016-5855
- CVE-2017-0632
- CVE-2017-0633
- CVE-2017-0634
- CVE-2017-2522
- CVE-2017-2523
- CVE-2017-2497
- CVE-2017-6981
- CVE-2017-6979
- CVE-2017-2051
- CVE-2017-2507
- CVE-2017-6987
- CVE-2017-7004
- CVE-2017-2513
- CVE-2017-2518
- CVE-2017-2520
- CVE-2017-2519
- CVE-2017-6983
- CVE-2017-6991
- CVE-2017-7000
- CVE-2017-7001
- CVE-2017-7002
- CVE-2017-2524
- CVE-2017-2496
- CVE-2017-2505
- CVE-2017-2506
- CVE-2017-2514
- CVE-2017-2515
- CVE-2017-2521

- CVE-2017-2525
- CVE-2017-2526
- CVE-2017-2530
- CVE-2017-2531
- CVE-2017-2538
- CVE-2017-2539
- CVE-2017-2544
- CVE-2017-2547
- CVE-2017-6980
- CVE-2017-6984
- CVE-2017-2504
- CVE-2017-2508
- CVE-2017-2510
- CVE-2017-2528
- CVE-2017-2536
- CVE-2017-2549
- CVE-2017-2499
- CVE-2016-7056
- CVE-2017-0603
- CVE-2016-10294
- CVE-2017-0615
- CVE-2017-0617

Possible Countermeasures

Enterprise

Deploy MAM or MDM solutions with policies that prohibit the side-loading of apps, which may bypass security checks on the app.

Deploy MAM or MDM solutions with policies that prohibit the installation of apps from 3rd party (unofficial) app stores.

Use application threat intelligence data to identify apps that exploit the OS to achieve privilege escalation.

Use app-vetting tools or services to identify apps that exploit the OS to achieve privilege escalation.

To limit the opportunity for malicious apps to exploit known vulnerabilities, ensure timely installation of security updates.

Mobile Device User

Use the Android Verify Apps feature to identify potentially harmful apps.

To limit the opportunity for malicious apps to exploit known vulnerabilities, ensure timely installation of security updates.

References
