EMM-5 · Mobile Threat Catalogue

Archived: 2026-04-06 01:53:22 UTC

Mobile Threat Catalogue

Bypassing Root/Jailbreak Checks

Contribute

Threat Category: Enterprise Mobility

ID: EMM-5

Threat Description: Root and jailbreak detection for mobile devices is based on detecting the changes that a process by which a mobile device was compromised would have caused. For instance, creation of files or directories that do not exist on uncompromised devices. Given the diversity of mobile devices, mobile OSs, the varying methods of compromise, and the potential for an attacker to intercept and forge acceptable responses to checks for such changes, root detection continues to be an area of challenge.

Threat Origin

All Your Root Checks Are Belong to Us: The Sad State of Root Detection [1]

Exploit Examples

Not Applicable

CVE Examples

- CVE-2017-4895

Possible Countermeasures

Enterprise

To increase the potential that device root or jail-break is detected, deploy a variety of mechanisms capable of root or jail-break detection (e.g., on-device agents, apps that require successful boot attestation checks, manual inspection)

To reduce the opportunity for an attacker to locally root or jail-break devices, educate users on the importance of physically securing their devices (e.g., locking it into a container) when not directly attended.

To reduce the potential a given root or jail-break attack will succeed, ensure devices are configured with a strong device unlock code.

Mobile Device User

To reduce the potential for USB-based root or jail-break exploits, do not accept prompts to grant trust when connecting to untrusted computers or charging stations.

References

1. N.S. Evans, A. Benameur, and Y. Shen, “All Your Root Checks Are Belong to Us: The Sad State of Root Detection”, in Proceedings of the 13th ACM International Symposium on Mobility Management and Wireless Access, 2015, pp. 81-88; http://dx.doi.org/10.1145/2810362.2810364 [accessed 8/23/2016] ↩
