# CVE Detail – CVE-2017-0492

An elevation of privilege vulnerability in the System UI could enable a local malicious application to create a UI overlay covering the entire screen. This issue is rated as Moderate because it is a local bypass of user interaction requirements that would normally require either user initiation or user permission. Product: Android. Versions: 7.1.1. Android ID: A-30150688.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.25371

## CVSS Scoring

CVSS v3.0 Score: 5.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-1021: Improper Restriction of Rendered UI Layers or Frames

## CAPEC(s)

* CAPEC-103: Clickjacking
* CAPEC-181: Flash File Overlay
* CAPEC-222: iFrame Overlay
* CAPEC-504: Task Impersonation
* CAPEC-506: Tapjacking
* CAPEC-587: Cross Frame Scripting (XFS)
* CAPEC-654: Credential Prompt Impersonation

## ATT&CK Techniques

* T1036.004: Masquerade Task or Service
* T1548.004: Elevated Execution with Prompt
* T1056: Input Capture

## Used By (Actors/Tools)

* Exaramel for Windows (malware)
* StrongPity (malware)
* Nebulae (malware)
* RainyDay (malware)
* TinyTurla (malware)
* Emotet (malware)
* Turian (malware)
* Machete (malware)
* PingPull (malware)
* Mafalda (malware)
* Hildegard (malware)
* FlawedAmmyy (malware)
* InvisiMole (malware)
* Volgmer (malware)
* RDAT (malware)
* Okrum (malware)
* Raspberry Robin (malware)
* Fysbis (malware)
* DCSrv (malware)
* ShimRat (malware)
* Green Lambert (malware)
* GoldMax (malware)
* PlugX (malware)
* Truvasys (malware)
* SVCReady (malware)
* Chaes (malware)
* Uroburos (malware)
* Spica (malware)
* KONNI (malware)
* Shamoon (malware)
* Black Basta (malware)
* Catchamas (malware)
* Attor (malware)
* NightClub (malware)
* Crutch (malware)
* RTM (malware)
* RawPOS (malware)
* ZxxZ (malware)
* Tarrask (malware)
* Bazar (malware)
* Kobalos (malware)
* SUGARDUMP (malware)
* Nidiran (malware)
* OSX\_OCEANLOTUS.D (malware)
* Seasalt (malware)
* FunnyDream (malware)
* SysUpdate (malware)
* Kwampirs (malware)
* DEADEYE (malware)
* InnaputRAT (malware)
* Egregor (malware)
* build\_downer (malware)
* Meteor (malware)
* Maze (malware)
* ComRAT (malware)
* metaMain (malware)
* Heyoka Backdoor (malware)
* KillDisk (malware)
* POWERSTATS (malware)
* OSX/Shlayer (malware)
* DEADWOOD (malware)
* SLOTHFULMEDIA (malware)
* NPPSPY (tool)
* CSPY Downloader (tool)
* IronNetInjector (tool)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* APT41 DUST (campaign)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* APT42 (intrusion-set)
* FIN6 (intrusion-set)
* Magic Hound (intrusion-set)
* APT39 (intrusion-set)
* APT32 (intrusion-set)
* BackdoorDiplomacy (intrusion-set)
* Kimsuky (intrusion-set)
* Storm-1811 (intrusion-set)
* RedDelta Modified PlugX Infection Chain Operations (campaign)
* BITTER (intrusion-set)
* APT41 (intrusion-set)
* FIN13 (intrusion-set)
* Versa Director Zero Day Exploitation (campaign)
* Frankenstein (campaign)
* Higaisa (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* ZIRCONIUM (intrusion-set)
* Naikon (intrusion-set)
* C0017 (campaign)
* Winter Vivern (intrusion-set)
* 2022 Ukraine Electric Power Attack (campaign)
* Carbanak (intrusion-set)
* KV Botnet Activity (campaign)
* APT-C-36 (intrusion-set)
* PROMETHIUM (intrusion-set)

## Affected Products

* cpe:2.3:o:google:android:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:google:android:7.1.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:google:android:7.1.1:\*:\*:\*:\*:\*:\*:\*