National Cyber Security Centre

2009161729-NCSC

A part of **Department of Communications, Climate Action & Environment**

NCSC Flash Alert

Critical Vulnerabilities in MobileIron
2020-09-16

Status: TLP-WHITE

NCSC

Threat Type	The vulnerability researcher Orange Tsai from DEVCORE has reported a number of vulnerabilities in MobileIron Core. More details can be found here.
	
	• CVE-2020-15505 - Remote Code Execution
	  – A remote code execution vulnerability in MobileIron Core and Connector versions 10.6 and earlier, and Sentry versions 9.8 and earlier that allows remote attackers to execute arbitrary code via unspecified vectors.
	• CVE-2020-15507 - Arbitrary File Reading
	  – An arbitrary file reading vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to read files on the system via unspecified vectors.
	• CVE-2020-15506 - Authentication Bypass
	  – An Authentication Bypass vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to bypass authentication mechanisms via unspecified vectors.

Products Affected	These vulnerabilities affect the following MobileIron products. • MobileIron Core • MobileIron Sentry • MobileIron Cloud • Enterprise Connector • Reporting Database (RDB)
Impact	Unauthenticated Remote Code Execution.
Recommendations	NCSC-IE recommends that affected organisations should apply the appropriate updates or workarounds as recommended by MobileIron as soon as possible. MobileIron customers can access patches here.