nomasis
secures your mobility

Why companies should protect their smartphones and tablets

February 2024

Why companies should protect their smartphones and tablets

By Patrick Trevisan - Mobile Security Consultant - Nomasis AG

For decades, companies have protected their PCs and laptops with antivirus programmes, firewall settings, VPN connections and other protection mechanisms. For smartphones and tablets, they continue to rely on the operating system architecture and mobile device management systems, although most attacks on company data, infrastructures and individuals nowadays start with smartphones and tablets.

Mobile Threat Defence (MTD) solutions for smartphones and tablets have been on the market for around 20 years and offer protection against phishing, network attacks, app risks and other threats. But most companies only invest in such insurance when it is too late.

Smartphones and tablets: an open barn door for attackers

Apple and Android smartphones and tablets have been finding their way into companies for several years now and the number is constantly increasing as part of 'modern work' and 'work from anywhere'. Whether simply for synchronising email, calendars and contacts or for accessing CRM, SAP, company applications and other services, these devices have become an indispensable and efficient tool in the modern working world.

Of course, malicious attackers have also recognised this. On the one hand, these devices contain a wealth of information such as passwords, credit cards, personal and company information and other data useful for espionage and criminal activities. On the other hand, access to the camera, microphone and other sensors is no longer a utopian dream, as recent attacks on well-known companies and institutions have shown.

It is also important to note that companies allow the private use of their smartphones and tablets or pursue a bring-your-own-device (BYOD) strategy. This increases the attack vector many times over, as phishing attacks, for example, can also reach the device from private emails, text messages and apps.

It is therefore all the more surprising that many companies still assume that they are sufficiently protected with a mobile device management (MDM) system and the operating system architecture of Apple iOS/iPadOS and Google Android. They do not realise that smartphones and tablets are the weakest links in their device fleet without the appropriate additional security measures and represent latent attack vectors for criminals.

MDM systems manage mobile devices and only offer basic IT protection

An MDM system enables the simple integration, inventory and management of mobile devices. Although MDM provides a good and important basis for the operation and protection of mobile devices in companies, it offers very deep basic protection in terms of IT security. This basic IT protection is limited to the following functions:

- Promotion of a device PIN or biometrics
- Rudimentary security guidelines regarding OS versions
- Rudimentary guidelines regarding app blacklisting
- Guidelines regarding data loss prevention
- Protection against jailbreaks/root access initiated by the user

MDM systems offer no protection against the following risks:

- Phishing attacks
- Malware
- Sideloading of apps
- Apps with weak or malicious code
- Network attacks (e.g. man-in-the-middle)
- Hidden jailbreaks/root access
- Early detection of new threats

The Android and iOS/iPadOS operating system is secure... or is it?

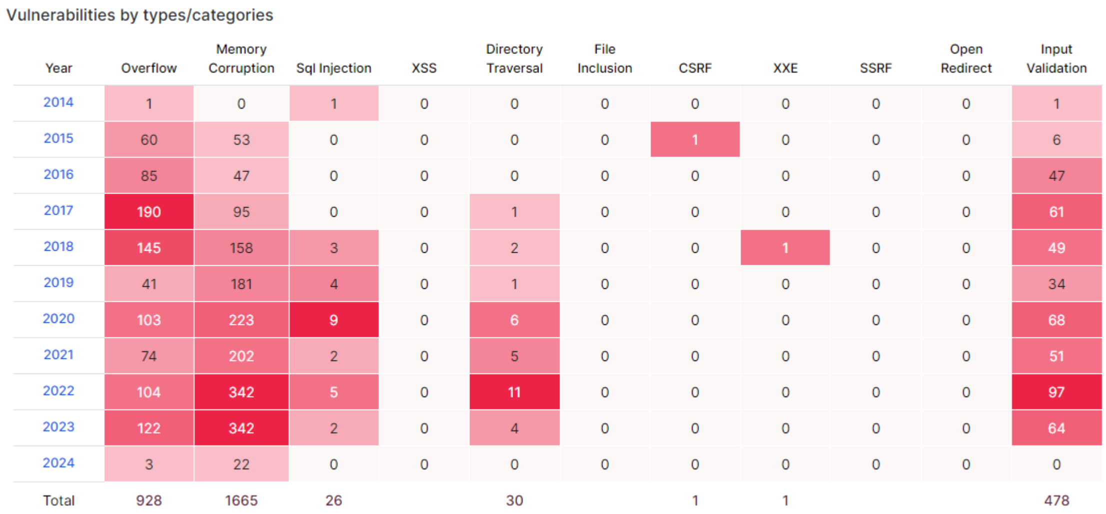
If you take a closer look at the statistics on attacks and attack vectors, you quickly realise that Apple and Google are also constantly working to close vulnerabilities and security holes in their operating systems and app frameworks.

Just like Microsoft for Windows, Apple and Google release regular security updates and hotfixes for iOS and Android, which close security gaps and incorporate new functionalities to ensure security.

It should also be noted that these platforms are usually located outside the company perimeter and connect to company data via unknown WiFi or data network connections. In addition, many data backends are now located in the cloud, which requires additional communication security, even on mobile devices.

Below are statistics from cvedetails.com on the individual device platforms and their known vulnerabilities:

Google Android

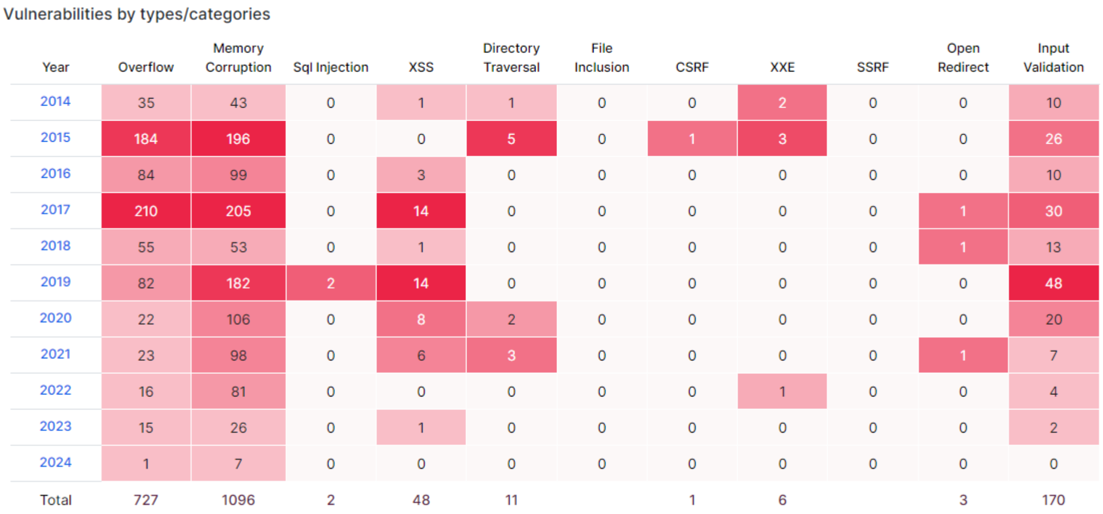


Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	1	0	1	0	0	0	0	0	0	0	1
2015	60	53	0	0	0	0	1	0	0	0	6
2016	85	47	0	0	0	0	0	0	0	0	47
2017	190	95	0	0	1	0	0	0	0	0	61
2018	145	158	3	0	2	0	0	1	0	0	49
2019	41	181	4	0	1	0	0	0	0	0	34
2020	103	223	9	0	6	0	0	0	0	0	68
2021	74	202	2	0	5	0	0	0	0	0	51
2022	104	342	5	0	11	0	0	0	0	0	97
2023	122	342	2	0	4	0	0	0	0	0	64
2024	3	22	0	0	0	0	0	0	0	0	0
Total	928	1665	26		30		1	1			478

Source and further details

Apple iPhone OS

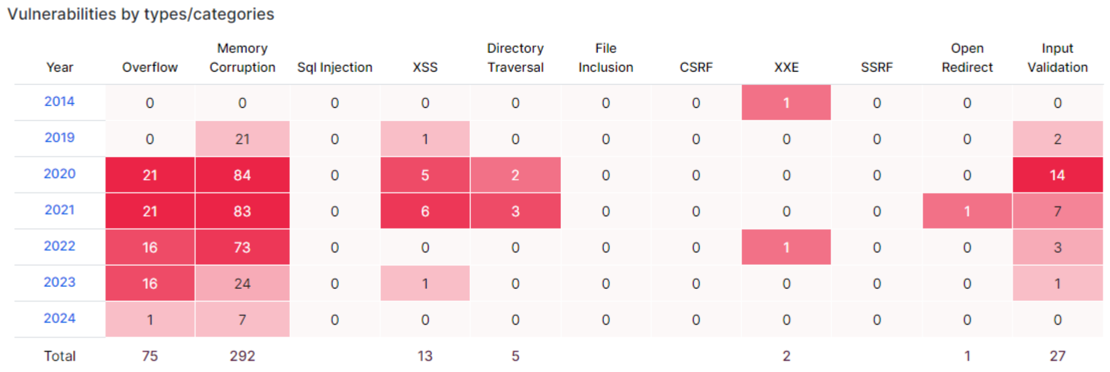


Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	35	43	0	1	1	0	0	2	0	0	10
2015	184	196	0	0	5	0	1	3	0	0	26
2016	84	99	0	3	0	0	0	0	0	0	10
2017	210	205	0	14	0	0	0	0	0	1	30
2018	55	53	0	1	0	0	0	0	0	1	13
2019	82	182	2	14	0	0	0	0	0	0	48
2020	22	106	0	8	2	0	0	0	0	0	20
2021	23	98	0	6	3	0	0	0	0	1	7
2022	16	81	0	0	0	0	0	1	0	0	4
2023	15	26	0	1	0	0	0	0	0	0	2
2024	1	7	0	0	0	0	0	0	0	0	0
Total	727	1096	2	48	11		1	6		3	170

Source and further details

Apple iPad OS



Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	0	0	0	0	0	0	0	1	0	0	0
2019	0	21	0	1	0	0	0	0	0	0	2
2020	21	84	0	5	2	0	0	0	0	0	14
2021	21	83	0	6	3	0	0	0	0	1	7
2022	16	73	0	0	0	0	0	1	0	0	3
2023	16	24	0	1	0	0	0	0	0	0	1
2024	1	7	0	0	0	0	0	0	0	0	0
Total	75	292		13	5			2		1	27

Source and further details

Mobile Threat Defence (MTD): concrete IT protection for mobile devices

As mentioned at the beginning, there have always been solutions on the market that protect against threats on mobile device platforms just as well as the solutions we have always used on PCs and laptops. These solutions are called Mobile Threat Defence or MTD for short and offer complementary IT security for mobile device platforms with regard to the following risks and entry points:

- Network
    - Unsecured WiFi networks or hotspots
    - Man-in-the-middle attacks
- Apps
    - Personal and company apps
    - Apps that disclose or transfer data
    - Side-loading or malicious apps
    - Poorly coded apps
    - Outdated apps
- Web & Content
    - Phishing attacks
    - Scanning QR codes
    - Harmful web content
- Device
    - Hidden jailbreaks and root access
    - Outdated operating systems
- Early detection of new threats in all areas

Such MTD solutions are generally based on a machine learning database and regularly scan millions of devices and apps without violating the privacy of users, detect anomalies and, depending on the configured security or intervention policy, can trigger appropriate measures such as blocking access or even decommissioning the device.

Most solutions also offer integration with existing MDM, IAM and SIEM infrastructures. This allows SOC employees to monitor the security of the mobile device fleet and intervene if necessary.

Nomasis protects you, your end users and your device fleet as part of its Nomasis Mobile Threat Defence Management Services in cooperation with well-known MTD manufacturers. Click here for more information.