Govt issues warning for Samsung phones

Flags multiple vulnerabilities, emphasises need for urgent updates

ASHUTOSH MISHRA
New Delhi, 15 December

The Centre's nodal agency for cyber security, Indian Computer Emergency Response Team (Cert-In), has issued a high-risk warning for Samsung smartphones, flagging multiple vulnerabilities and emphasising the need for urgent updates of their operating systems.

The alert highlights security concerns and asserts that the phones are prone to vulnerabilities that can allow an attacker to snoop and access data on the device without the user's knowledge.

"Multiple vulnerabilities have been reported in Samsung products which could allow an attacker to bypass implemented security restrictions, access sensitive information and execute arbitrary code on the targeted system," read the Cert-In advisory issued this week. It highlighted that these vulnerability issues might affect Samsung phones running on Android versions 11 and above.

"These vulnerabilities exist due to improper access control flaw in Knox Custom Manager Service and Smart Manager CN component, integer overflow vulnerability in face pre-processing library; improper authorisation verification vulnerability in AR emoji, improper exception management vulnerability in Knox Guard, various out of bounds write vulnerabilities in bootloader, HDCP in HAL, libIfaaCa and libsavsac.so components, improper size check vulnerability in softsimd, improper input validation vulnerability in Smart-Clip and implicit intent hijacking vulnerability in contacts," read the detailed statement.

The exploitation of these vulnerabilities may allow an attacker to trigger heap overflow and stack-based buffer overflow, access device SIM PIN, send broadcast with elevated privilege, read sandbox data of AR Emoji, bypass Knox Guard lock via changing system time, access arbitrary files, gain access to sensitive information, execute arbitrary code and compromise the targeted system, the agency said.

Cert-In has advised users to apply appropriate security patches released by Samsung to prevent their devices from risk. Meanwhile, Samsung Mobile has announced the rollout of a maintenance release as part of its December 2023 security update.

"Samsung Mobile is releasing a maintenance release for major flagship models as part of the monthly Security Maintenance Release (SMR) process. This SMR package includes patches from Google and Samsung," said the South Korean smartphone major on its website.

Cert-In, the national nodal agency under the Ministry of Electronics and Information Technology, is tasked with responding to computer security incidents as and when they occur. The agency has been flagging security threats and risks associated with the cybersecurity domain and had recently issued a high-severity rated warning cautioning against "multiple vulnerabilities" in the web browser Google Chrome, which could allow a remote attacker to execute arbitrary code and cause denial of service conditions on targeted systems.

SAFETY MEASURES

- Cert–In issued a high severity risk warning to Samsung users, asking users to update their devices
- Can impact Samsung phones running on Android versions 11 and above
- The agency also pointed out vulnerabilities in different software elements including Knoxguard and AR emoji features
- Attackers can bypass security restrictions, gain unauthorised access to sensitive information
- Samsung has announced the roll out of a maintenance release as part of its December security update
- Cert–In had recently issued a high–severity rated warning cautioning against "multiple vulnerabilities" in web browser Google Chrome