Hackers spent 2+ years looting secrets of chipmaker NXP before being detected

By Dan Goodin

Published: 2023-11-28 · Archived: 2026-04-05 18:33:07 UTC

“NXP chips are in a lot of products,” Jake Williams, a former hacker for the National Security Agency, wrote on Mastodon. “It’s likely the TA knows of specific flaws reported to NXP that can be leveraged to exploit devices the chips are embedded in, and that’s assuming they didn’t implement backdoors themselves. Over 2.5 years (at least), that’s not unrealistic.”

A separate researcher who has published research in the past documenting a successful hack on a widely used product containing NXP chips voiced similar surprise.

“If a Chinese threat actor group gets source code or hardware designs of a chip manufacturer, these kinds of groups can use the source code even if the source code isn’t very well commented and documented,” the researcher, who asked not to be identified, said in an interview. “For me, [the intrusion] is a big deal. I was surprised NXP didn’t communicate with its customers.”

In an email, an NXP representative said the NRC report “is very dated as it was addressed back in 2019. As stated in our 2019 Annual Report, we became aware of a compromise of certain IT systems, and after a thorough investigation we determined that this incident did not result in a material adverse effect on our business. At NXP, we take the security of data very seriously. We learned from this experience and prioritize continually strengthening our IT systems to protect against ever-evolving cybersecurity threats.”

Chimera has extensive experience stealing data from a wide range of companies. The threat actor uses a variety of means to compromise its victims. In the campaign that hit NXP, hackers often leveraged account information revealed in previous data breaches of sites such as LinkedIn or Facebook. The data allowed Chimera to guess the passwords that employees used to access VPN accounts. Team members were able to bypass multi-factor authentication by changing telephone numbers associated with the accounts.

Security firm Cycraft documented one two-year hacking spree that targeted semiconductor makers with operations in Taiwan, where NXP happens to have research and development facilities. An attack on one of the unnamed victims compromised 10 endpoints and another compromised 24 endpoints.

“The main objective of these attacks appeared to be stealing intelligence, specifically documents about IC chips, software development kits (SDKs), IC designs, source code, etc.,” Cycraft researchers wrote. “If such documents are successfully stolen, the impact can be devastating.”
