مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

PKfail: Secure Boot Bypass Vulnerability

Tracking #:432316098

Date:29-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a significant vulnerability known as "PKfail" has been identified, compromising Secure Boot functionality on over 200 models.

TECHNICAL DETAILS:

This vulnerability arises from poor cryptographic key management practices, specifically the leakage of a critical platform key (PK) protected by an easily guessable four-character password. As a result, attackers can bypass Secure Boot protections, exposing devices to sophisticated malware attacks, including persistent boot kits.

Vulnerability Details:

- **Vulnerability Name**: PKfail
- **Affected Models**: Over 200 models from manufacturers such as Acer, Dell, Intel, and Supermicro.
- **Key Management Issue**: The platform key (PK) was leaked and is protected by a weak password, allowing unauthorized access.
- **Potential Impact**: Devices can be compromised by boot kits, leading to persistent malware infections that evade traditional antivirus solutions. Scope: Affects various device types, including consumer laptops, servers, and industrial systems.
- **Mitigiation**: Addressing PKfail requires rekeying on affected devices the Platform Key with a new trusted key. Devices affected by PKfail must be assumed compromised and thus KEK, db and dbx must also be checked and replaced with new databases of trusted signatures and certificates.

RECOMMENDATIONS:

- **Immediate Device Assessment**: Conduct an inventory of all devices within your organization to identify models affected by the PKfail vulnerability.
- **Firmware Updates**: Monitor for firmware updates from manufacturers addressing the PKfail vulnerability.
- **Enhanced Security Measures**: Implement additional security layers, such as endpoint detection and response (EDR) solutions, to monitor for unusual activity on devices.
- **Cryptographic Key Management**: Establish strict protocols for managing cryptographic keys, including regular audits and key rotation practices.
- **User Awareness and Training**: Conduct training sessions for employees on recognizing phishing attempts and other social engineering tactics that could lead to device compromise.
- **Incident Response Planning**: Review and update incident response plans to include scenarios involving compromised Secure Boot functionality.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.binarly.io/advisories/brly-2024-005-usage-of-default-test-keys-leads-to-complete-secure-boot-bypass