DUHK attacks allow hackers to obtain encryption keys for VPN and web browsing sessions

DUHK - Dont Use Hard-coded Keys - is a new dangerous encryption executable vulnerability that allows an attacker to recover the encryption key used to secure VPN connections and web sessions.

DUHK - Dont Use Hard-coded Keys - is a new dangerous encryption executable vulnerability that allows an attacker to recover the encryption key used to secure VPN connections and web sessions.

DUHK is the third vulnerability related to encryption discovered this month, after attacking WiFi KRACK and attacking ROCA.

This vulnerability exists on many devices of many vendors, including Fortinet, Cisco, TechGuard, where the device uses ANSI X9.31 RNG - an algorithm to generate pseudo random numbers - along with the key hard-coded (just embedding it directly into source or fixed data instead of taking from external sources).

Before being removed from the list of FIPS-approved random number sequence algorithms approved in January 2016, ANSI X9.31 RNG is used in many coding standards for more than 30 years.

The pseudo random number generator (PRNG) does not generate random numbers. In essence, it is an algorithm that creates a series of bits based on secret values ??originally called 'seeds' and creates the current state. This bit sequence is always the same due to the same initial values.

Some vendors store this 'secret seed' into their product source code.

Discovered by cryptanalysts Shaanan Cohney, Nadia Heninger and Matthew Green, DUHK, known as 'status restoration attack', allows intermediaries who already know the value of seeds restore the current value after viewing the output data.

With those two values, the attacker uses to recalculate the encryption key, restoring the encrypted data.

'To describe the reality, we created passive decoding attack on FortiGate VPN product with FortiOS version 4', the researchers said. 'We scanned at least 23,000 devices with public IPv4 addresses running FortiOS versions containing vulnerabilities'. Below is an incomplete list of influential devices with the same version.

Vendor	Product Line	Version
BeCrypt Ltd.	BeCrypt Cryptographic Library	2.0
Cisco Systems Inc	Aironet	7.2.115.2
Deltacrypt Technologies Inc	DeltaCrypt FIPS Module	
Fortinet Inc	FortiOS v4	4.3.17
MRV Communications	LX-4000T/LX-8020S	v5.3.8
Neoscale Systems Inc	CryptoStor	2.6
Neopost Technologies	Postal Security Devices	v28.0
Renesas Technology America	AE57C1	v2.1012
TechGuard Security	PoliWall-CCF	v2.02.3101
Tendyron Corporation	OnKey193	v122.102
ViaSat Inc	FlagStone Core	v2.0.5.5
Vocera Communications Inc.	Vocera Cryptographic Module	v1.0

Vendor products containing vulnerabilities are vulnerable to DUHK attacks

Researchers have also published in-depth research material on the DUHK attack website at this address. *https://duhkattack.com/*