IOActive Security Advisory

Title	Physical and Authentication Bypass in Diebold Opteva ATM
Severity	Critical
Discovered by	Mike Davis, Josh Hammond
Advisory Date	July 26, 2017

Affected Products

Some versions of Diebold's Opteva Automated Teller Machines (ATMs) and Advanced Function Dispenser (AFD) platform

Impact

IOActive has discovered two vulnerabilities in Opteva ATMs with the AFD platform that, when combined, may allow an unauthorized user to vend notes from the device.

Background

Historically, ATMs have been designed without privileged separation between the safe and the internal operating system. In an attempt to address this security concern, Diebold developed the AFD platform. The Opteva line of ATMs with the AFD platform contain an upper cabinet for the operating system and a lower cabinet for the safe, each with its own authentication requirements.

Using reverse engineering and protocol analysis, IOActive found a critical vulnerability in the tested version of the Opteva ATM with the AFD platform. Despite its separation of privilege and authentication requirements, the ATM is still vulnerable to a malicious attacker, compromising its integrity and causing unauthenticated vending from the AFD.

Technical Details

IOActive researchers began by physically compromising the device. Using a metal rod inserted through a speaker hole on the front of the ATM, the researchers were able to lift a metal locking bar to gain access to the upper cabinet of the ATM, which contains the computer. Once the research team had access to the cabinet, they removed the USB connection from the Windows host and gained a direct line of communication to the AFD controller within the safe.

With access to the upper cabinet and the operating system's firmware, IOActive researchers determined that another vulnerability would be necessary to gain access to the contents of the safe. Since the AFD governs the security of the safe, IOActive reverse engineered the AFD's protocol and firmware.

Using the USB that connects the AFD to the computer in the upper cabinet, the team was able to initiate two-way communication. This would normally require a shared encryption key and a device identifier; however, the team was able to complete the authentication protocol unencrypted and set up communications without properly authenticating. This allowed the team to act as an authenticated user and gain access to the contents of the safe.

The protocol does not require any device specific knowledge to carry out the attack. This would imply that an attacker with access to one device could reverse engineer enough of the controller protocol to effectively bypass authentication and vend notes from any other device that uses an AFD as long as the vulnerability remains unpatched.

Proof-of-Concept

Figure 1 shows the expected flow of the AFD platform: the communication is encrypted with a pre-shared key and requires a device ID to finish a hash.

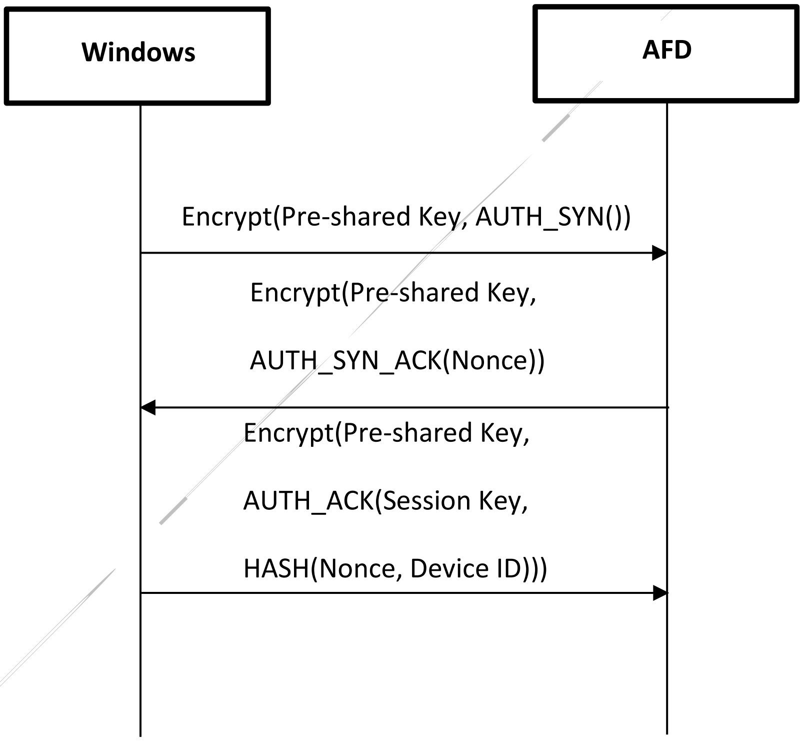

Figure 1. AFD platform expected flow

Figure 2 shows what IOActive researchers found: the encryption and device ID are optional.

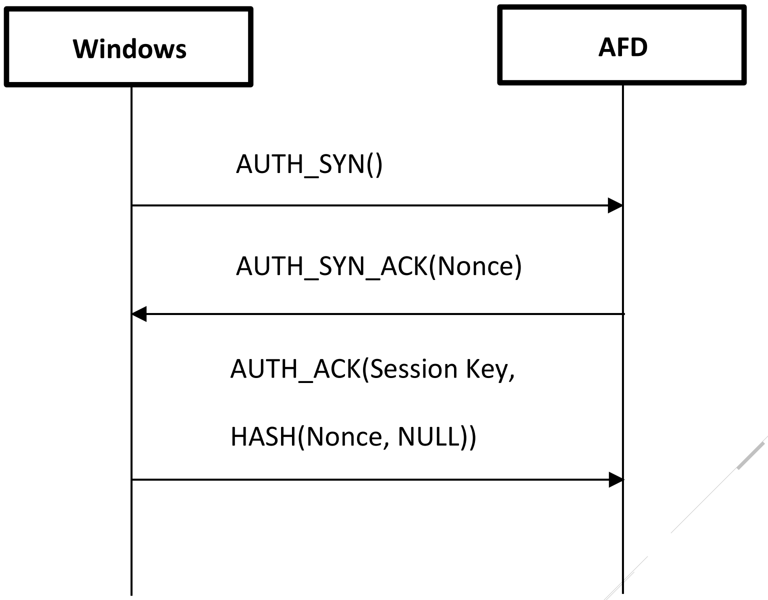

Figure 2. AFD platform acceptable flow

Mitigation

IOActive recommends that the manufacturer patch their firmware to ensure the encryption flag is always set and the hash containing the device ID is always verified. Enforcing these measures prevents an attacker from bypassing authentication.

Fixes

IOActive initially worked with Diebold to disclose the vulnerabilities and clairify the effected systems. Diebold has confirmed receipt of IOActive's information disclosure; however, Diebold has not informed IOActive of any actions they have taken, if affected systems exist, or what versions and configurations remain vulnerable to these issues.

Timeline

Feb 17, 2016	Initial contact and disclosure of physical bypass
Mar 4, 2016	Diebold requests more information
Jan 17, 2017	Initial attempt to contact Diebold regarding software bypass
Jan 18, 2017	Diebold responds
Jan 19, 2017	Diebold provides secure transit for disclosure
Jan 25, 2017	Diebold acknowledges disclosure
Jan 30, 2017	Diebold requests a discussion regarding the disclosure
Feb 13, 2017	Conference call; Diebold requests AMI tracelogs to determine version information
Feb 15, 2017	IOActive provides tracelogs
Mar 14, 2017	IOActive attempts follow-up
Mar 26, 2017	IOActive attempts follow-up
Mar 28, 2017	IOActive attempts follow-up
Apr 1, 2017	Primary contact is reportedly on vacation, "will follow up this week"
May 19, 2017	IOActive attempts follow-up
Mar 22, 2017	Diebold responds, "[your]..system is very old (2008/2009 vintage) and is unpatched;" IOActive asks if retesting a recent supported version would be possible
Mar 24, 2017	IOActive asks if "2008/2009" are usable as version numbers, and whether Diebold had patched this specific issue; IOActive extends an offer to retest current firmware with the stipulation that this version is not a patch addressing the specific issue reported by IOActive
Jun 19, 2017	IOActive attempts follow-up
Jul 26, 2017	IOActive disclosure