



VULNERABILITY REPORT 1721

1st September 2023

FIDO2 NFC Authenticator Vulnerability

Report on potential FIDO2 Vulnerability related during independent pentest.

INTRODUCTION


This vulnerability was discovered by 2 researchers, who presented it in their research article titled “FIDO2: The Phishing resistant authentication standard, or is it phishable”.

The research specifically targeted FIDO2 NFC authenticators and proves that given a combination of social engineering scenarios, thanks to a malware that controls NFC interface of a smartphone used as a NFC reader, an attacker could impersonate the user. The researchers are Aditya Mitra and Anisha Ghosh.

DISCLAIMER

Recipients may share this paper with peers and partner organizations. Information in this paper can be circulated within the FIDO Alliance community. Information contained in this document may be released outside of FIDO Certification Secretariat, the Researcher in question, FIDO Accredited Labs and the SRWG in the FIDO Alliance.

REVISION HISTORY

Revision	Date	Description	Triage Level
V1.0	1 st September 2023	Initial version	GREEN 

VULNERABILITY INFORMATION

This vulnerability exploits authenticator's NFC communication and CTAP protocol to impersonate a user. This is done through a complex phishing scenario where a mobile phone used as an NFC reader by the legitimate user is compromised.

AFFECTED SOFTWARE/HARDWARE

All FIDO authenticators (FIDO) implementing NFC and CTAP (version 2.0 and 2.1) as a means of connecting to carry out an authentication related operation

ATTACK COMPLEXITY (Methods, Techniques and Tools)

Method

The scenario target the CTAP protocol used to communicate between the client (e.g. the user's browser) and the authentication (USB, NFC or BLE device). In particular, these attacks have been performed only on NFC authenticators. The exploit allows an adversarial actor to take over the account of the legitimate user without physically having access to the physical security key.

For this scenario to succeed, the attacker needs :

- the user to connect by performing an NFC tap with the authenticator on his mobile;
- to compromise the mobile where the authenticator is "tapped" to be able to manipulate the data exchanged through the NFC interface and put himself in MITM position.

From an attacker's perspective, there are a few steps required in order for a successful attack scenario to be achieved.

In the scenario presented here, the attack relies on the fact that the smartphone of the user is used as an NFC reader to authenticate the user on a service using FIDO. The attacker will put himself in a 'Man in the Middle' position between the browser and the NFC reader. He will use Personal Computer Smart Card API available on computer. This will allow him to connect his computer and therefore the authentication service running on his browser to an external NFC reader(here the victim's phone).

1. Attacker prepares the attack
 - a. Infect user smartphone: The user shall install a "fake NFC reader app" application on his phone. This application will relay NFC requests and response between the attacker's computer and the user's phone.
 - b. Mimic the service where user uses FIDO authentication.
2. Phish the user with the imitated service.
3. User enters his login information on the fake interface. This information is transmitted to the attacker. The attacker then enters user's login information on the real service.
4. The service asks for the FIDO authentication to the attacker's computer. This APDU command is automatically forwarded to the "fake NFC reader app" on the victim's phone.
5. The victim performs an NFC tap on his infected phone.
6. Exchanged information and validated challenges are transmitted to the attacker.
7. The computer of the attacker receives this data and transmits it to the service.
8. The attacker is logged in as the victim on the service.

VULNERABILITY TRIAGE

Background: Vulnerability Triage Criteria

The Vulnerability Triage Protocol is defined by the FIDO Authenticator Certification Program Policy¹.

See Table 1 below for the Triage Levels and Reasoning.

Triage Level	Triage Reasoning
RED	Attack in progress, or At-scale attacks exist that can be performed with readily available tools and limited skill.
AMBER	Vulnerability that is likely to lead to a scalable attack.
GREEN	Vulnerability where attack unlikely, or not scalable.
WHITE	Vulnerability that is outside the scope of FIDO Specifications.

Table 1: Vulnerability Triage Levels and Reasoning

¹ The latest version of the FIDO Authenticator Certification Program Policy can be found at: <https://fidoalliance.org/certification/authenticator-certification-levels/>.

Attack Potential Calculation

Security Vulnerability Calculated Attack Potential (IDENTIFICATION)		
Factor	Estimate	Value
Elapsed Time	<= one month	3
Expertise	Proficient	2
Knowledge of Target	Public	0
Windows of opportunity	Easy	1
Equipment	Specialized	1
Calculated Attack Potential		7

Security Vulnerability Calculated Attack Potential (EXPLOITATION)		
Factor	Estimate	Value
Elapsed Time	<= one day	2
Expertise	Layman	0
Knowledge of Target	Public	2
Windows of opportunity	Easy	1
Equipment	Specialized	3
Replicability	Difficult	6
Calculated Attack Potential		14

Total Attack Potential	21
------------------------	----

The attack potential required to exploit this attack is "Basic"

⇒ TOE must be resistant against **Enhanced-Basic** Attack Potential level.

Vulnerability Triage Level

- ⇒ Protocol (no software required) = **WHITE**
- ⇒ Specific FIDO implementations of the protocol or specific platforms only = **GREEN**
- ⇒ General authenticator vulnerabilities = **WHITE**
- ⇒ Specific vendor authenticator vulnerabilities = **WHITE**
- ⇒ Specific authenticator vulnerabilities related to a specific FIDO implementation = **WHITE**

CONCLUSION

Researchers showed that it's possible to trick someone into installing a malicious app on their phone. This app can then act like a relay, capturing the signals from the physical security key and passing them on to the attacker. This means the attacker could potentially log into the victim's account.

This vulnerability falls within the MiTMa family of vulnerabilities that affect the local communication between the browser and the authenticator.

The source of the vulnerability is clearly not the FIDO2 Authenticator but is related to the NFC functionalities and the user's device. This vulnerability implies that, if a malicious code finds its way to a user's device, the attacker could impersonate the user to access a RP account. This risk is carried by all FIDO2 NFC enabled devices. One of the assumptions considered in the FIDO protocol is for the computing environment on the FIDO user device and the end applications involved in a FIDO operation act as trustworthy agents of the user.

So, unfortunately, when smartphone user is compromised FIDO Authenticators do not have a way to fully resist against such new class of attacks alone. Basically, any strong authentication could be bypassed if someone tricks you into giving away all the authentication factors.

Hence the attack is judged to be not scalable and is more targeting the user's machine and not directly the Authenticator boundary (protocol and product) itself.