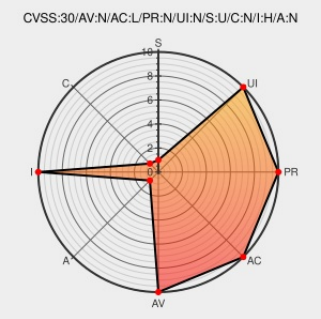
CVE-2018-12025

Published on: 06/11/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:24 PM UTC

CVE-2018-12025

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Futurxe from Futurxe contain the following vulnerability:

The transferFrom function of a smart contract implementation for FuturXE (FXE), an Ethereum ERC20 token, allows attackers to accomplish an unauthorized transfer of digital assets because of a logic error. The developer messed up with the boolean judgment - if the input value is smaller than or equal to allowed value, the transfer session would stop execution by returning false. This makes no sense, because the transferFrom() function should require the transferring value to not exceed the allowed value in the first place. Suppose this function asks for the allowed value to be smaller than the input. Then, the attacker could easily ignore the allowance: after this condition, the `allowed[from][msg.sender] -= value;` would cause an underflow because the allowed part is smaller than the value. The attacker could transfer any amount of FuturXe tokens of any accounts to an appointed account (the `_to` address) because the allowed value is initialized to 0, and the attacker could bypass this restriction even without the victim's private key.

CVE-2018-12025 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Bugged Smart Contract FuturXE: How Could Someone Mess up with Boolean? (CVE-2018–12025) | by p0n1 | SECBIT Media | Medium	Third Party Advisory medium.com text/html	MISC medium.com/secbit-media/bugged-smart-contract-f-e-how-could-someone-mess-up-with-boolean-d2251defd6ff

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Futurxe	Futurxe	-	All	All	All
Application	Futurxe	Futurxe	-	All	All	All

cpe:2.3:a:futurxe:futurxe:-:*:*:*:*:*:*:*:

cpe:2.3:a:futurxe:futurxe:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→