

Chaturya_19BCE7528_Pwndoc

VULNERABILITY REPORT

FRIDAY, JUNE 04, 2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/04/2021	Chaturya Chinta	Initial Version

TABLE OF CONTENTS

1.	General Information	4
1.1	Scope	4
1.2	Organisation	4
2.	Executive Summary	5
3.	Technical Details	6
3.1	title	6
4.	Vulnerabilities summary	8

GENERAL INFORMATION

SCOPE

undefined has mandated us to perform security tests on the following scope:

- Lab report of 19BCE7528

ORGANISATION

The testing activities were performed between 06/04/2021 and 06/04/2021.

EXECUTIVE SUMMARY

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-002	Directory Traversal Vulnerability	Vulnerable Versions: 3.36 and probably prior

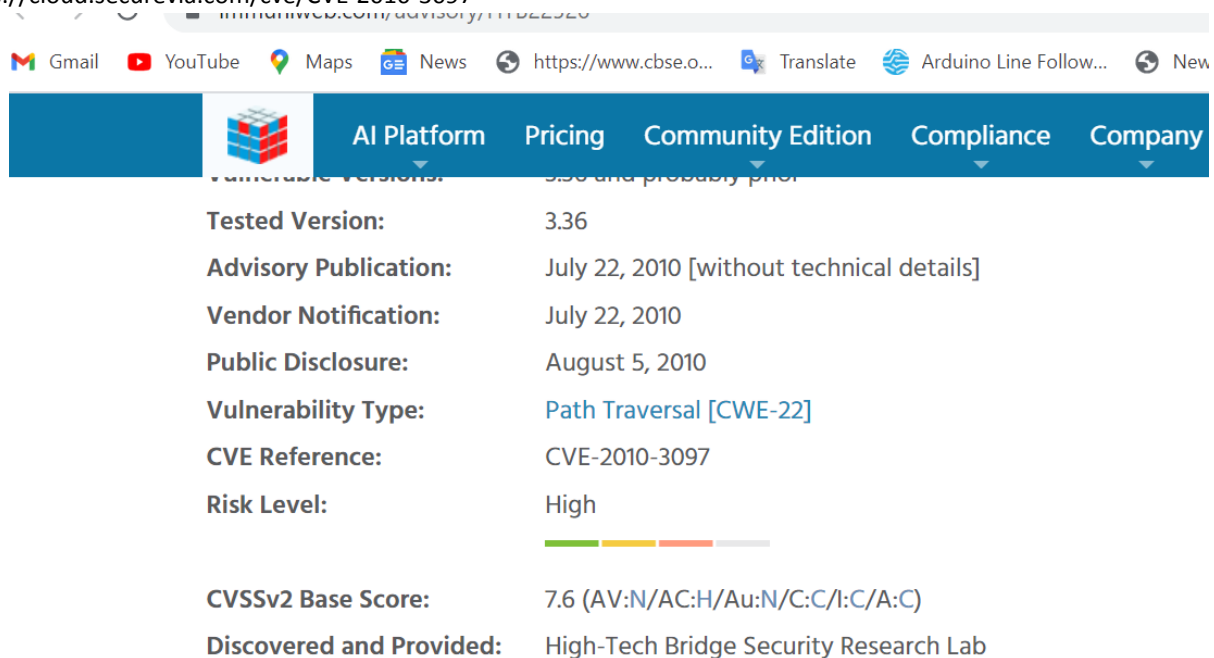
TECHNICAL DETAILS

DIRECTORY TRAVERSAL VULNERABILITY

CVSS SEVERITY	High	CVSSv3 SCORE	7.7
CVSSv3 CRITERIAS	Attack Vector : Network Attack Complexity : High Required Privileges : Low User Interaction : None	Scope : Changed Confidentiality : High Integrity : Low Availability : Low	
AFFECTED SCOPE	Vulnerable Versions: 3.36 and probably prior		
DESCRIPTION	High-Tech Bridge SA Security Research Lab has discovered vulnerability in Frigate 3 built-in FTP client which could be exploited to execute arbitrary code on vulnerable system. A vulnerability was found in WinFrigate Frigate 3 up to 3.17 and classified as critical. This issue affects an unknown code block. The manipulation with an unknown input leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is confidentiality, integrity, and availability.		
OBSERVATION	Directory Traversal Vulnerability in Frigate 3 FTP Client: CVE-2010-3097 The vulnerability exists due to insufficient sanitation of the downloaded filename. A remote attacker controlling an FTP server can trick user into downloading file with specially crafted filename, containing directory traversal sequences (e.g. "..\..\..\..\..\somefile.exe") and write it into arbitrary locations on the target system. Successful exploitation might allow remote code execution but requires that victim uses Frigate 3 FTP Client to connect to the FTP server and download a malicious file.		

TEST DETAILS

<https://cloud.securevia.com/cve/CVE-2010-3097>



[Gmail](#) [YouTube](#) [Maps](#) [News](#) <https://www.cbse.o...> [Translate](#) [Arduino Line Follow...](#) [New](#)

[AI Platform](#) [Pricing](#) [Community Edition](#) [Compliance](#) [Company](#)

Vulnerable Versions: 3.36 and probably prior

Tested Version: 3.36

Advisory Publication: July 22, 2010 [without technical details]

Vendor Notification: July 22, 2010

Public Disclosure: August 5, 2010

Vulnerability Type: [Path Traversal \[CWE-22\]](#)

CVE Reference: CVE-2010-3097

Risk Level: High

CVSSv2 Base Score: 7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

Discovered and Provided: High-Tech Bridge Security Research Lab

Image 1 – Official_Details.png	
REMEDIATION	Currently we are not aware of any vendor-supplied patches or other solutions. The vendor was contacted in accordance to our Vendor Notification Policy but we didn't get any answer or feedback.
REFERENCES	<p>1] High-Tech Bridge Advisory HTB22526 - https://www.immuniweb.com/advisory/HTB22526 - Directory Traversal Vulnerability in Frigate 3 FTP Client</p> <p>[2] Frigate3 - frigate3.com- Frigate3 is a handy file manager with wealth of options that make managing and browsing through files easy.</p> <p>[3] Common Vulnerabilities and Exposures (CVE) - http://cve.mitre.org/ - international in scope and free for public use, CVE® is a dictionary of publicly known information security vulnerabilities and exposures.</p> <p>[4] Common Weakness Enumeration (CWE) - http://cwe.mitre.org - targeted to developers and security practitioners, CWE is a formal list of software weakness types.</p>