



DeusSec

Deus Security Services

# Nitro Token Smart Contract

## Security Audit Report

December 9, 2021

<b><u>Introduction</u></b>	<b>2</b>
<b><u>Executive Summary</u></b>	<b>3</b>
<b><u>Overview</u></b>	<b>4</b>
Files in Scope	4
Project Summary	4
Severity Definition	4
Vulnerability Summary	5
Technical Summary	5
<b><u>Findings</u></b>	<b>6</b>
TM-01   Token Minted to Designated Address	6
<b><u>Disclaimer</u></b>	<b>7</b>



# Introduction

---

Deus Security Services (consultant) was contracted by Nitro-League (customer) to conduct smart contracts code review and security analysis.

This report presents the findings of the security assessment of customer's smart contracts and its code review conducted December 9, 2021. This audit report has been prepared for Nitro-League to discover and highlight issues and vulnerabilities in the Nitro-League project's source code and the overall security of the Nitro token. In this report, Deus Security Services, later DeusSec, attempts to ensure the reliability of the smart contract by completing recommended Static Analysis and Manual Review techniques.

The auditing assessment carried out by DeusSec pays special attention to the following considerations:

- Manual review of the entire codebase by industry experts
- Assessing the codebase to ensure compliance with current best practices
- Testing the smart contracts against both common and uncommon attack vectors.
- Ensuring contract logic meets the specifications and intentions of the client.
- Checking whether all the libraries used in the code are of the latest version.
- Running the tests and checking their coverage.

This report aims to help Nitro-League enhance general coding practices for better structures, correctness, and readability of source code. The audit verifies whether the smart contract is secure and working properly according to the specs. We recommend addressing the findings to ensure a high level of security standards and industry practices.

To evaluate the potential vulnerabilities or issues, we go through a checklist of well-known smart contract-related security issues using automatic verification tools and manual review.

DeusSec has discussed Nitro-League's business model to reduce the risk of unknown vulnerabilities. We might test it on our private network to reproduce the issue to prove our findings for any discovered issue.



# Executive Summary

---

The security state of the reviewed contract is "well secured" and is good to go for production.

According to the audit, the customer's Solidity smart contract is well secured and has no critical security problems. The audited contract uses the latest version of OpenZeppelin ERC20 token contract implementation, which is widely adopted and well audited by many parties in crypto community.

Our team reviewed all issues, which included the analysis of code functionality, manual review during automated analysis, and review of applicable vulnerabilities presented in the audit overview section.

The DeusSec team has also conducted unit tests using scripts provided through the same GitHub link, which fortifies the functionality and security of the contract, which also helped us determine the integrity of the code in an automated way.

Since possible test cases can be unlimited and developer-level documentation was not provided, we provide no guarantee of future outcomes. We have used all the latest static tools and manual observations to cover the maximum possible test cases.

Please read the whole document to estimate the risks reasonably.



# Overview

---

## Files in Scope

<https://github.com/Nitro-League/nitro>

Commit 0a7fc25241f3c873652bb6e438931061f4678621

## Project Summary

Nitro contract implements an ERC20 token standard.

## Severity Definition

**Critical.** The issue has the potential to result in data loss or asset manipulations.

**High.** The issue may seriously endanger the project's business model.

**Medium.** The issue requires a fix but doesn't pose a threat that is practical to exploit.

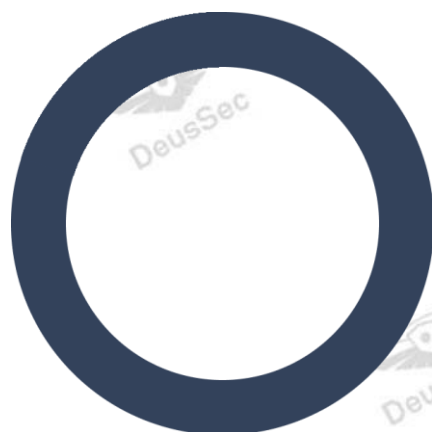
**Low.** The issue is likely related to outdated or unused code snippets.

**Informational.** The issue is stylistic; fixes are not mandatory.



# Vulnerability Summary

Severity	Total	Pending	Declined	Acknowledged	Resolved
Low	1	0	0	1	0



## Technical Summary

INDUSTRY STANDARD

YOUR RATING

0%

25%

50%

75%

100%

The tested smart contract code is 98%, which is above the industry standard of 95%



# Findings

ID	Title	Category	Severity	Status
TM-01	Token Minted to Designated Address	Control Flow	Low	Acknowledged

## TM-01 | Token Minted to Designated Address

ID	Category	Severity	Location	Status
TM-01	Control Flow	Low	nitro/contracts/Nitro.sol: 7	Acknowledged

### Description

The `constructor()` mints all of the tokens (1 Billion) to a single address ("distributor") with no checks.

### Recommendation

Please ensure the accuracy of the recipient address when calling the constructor of contract. We also advise the client to adopt Multisig, Timelock, and/or DAO in the project to manage this address.





# Disclaimer

---

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement.

This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without Deus Security Service's (from hereinafter DeusSec) prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts DeusSec to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technology's proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process, intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. DeusSec's position is that each company and individual are responsible for their own due diligence and continuous security.

DeusSec's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by DeusSec are subject to dependencies and under continuing development.





You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, DEUS SECURITY SERVICES (DEUSSEC) HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, DEUSSEC SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, DEUSSEC MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, DEUSSEC PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER DEUSSEC NOR ANY OF DEUSSEC'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. DEUSSEC WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.



ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT DEUSSEC'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST DEUSSEC WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF DEUSSEC CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST DEUSSEC WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR

ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

