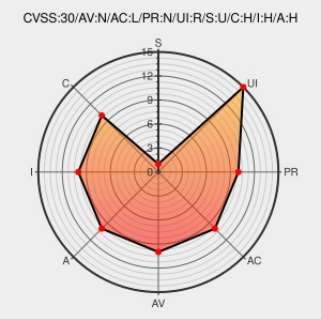
CVE-2018-3983

Published on: 10/31/2019 12:00:00 AM UTC

Last Modified on: 02/04/2023 01:22:00 AM UTC

CVE-2018-3983

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



Certain versions of Atlantis Word Processor from Atlantiswordprocessor contain the following vulnerability:

An exploitable uninitialized pointer vulnerability exists in the Word document parser of the the Atlantis Word Processor. A specially crafted document can cause an array fetch to return an uninitialized pointer and then performs some arithmetic before writing a value to the result. Usage of this uninitialized pointer can allow an attacker to corrupt heap memory resulting in code execution under the context of the application. An attacker must convince a victim to open a document in order to trigger this vulnerability.

CVE-2018-3983 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
TALOS-2018-0651 || Cisco Talos Intelligence Group	Exploit	MISC

TALOS-2018-0651 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	MISC	talosintelligence.com/vulnerability_reports/TALOS-2018-0651

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlantiswordprocessor	Atlantis Word Processor	3.0.2.3	All	All	All
Application	Atlantiswordprocessor	Atlantis Word Processor	3.0.2.5	All	All	All
Application	Atlantiswordprocessor	Atlantis Word Processor	3.0.2.3	All	All	All
Application	Atlantiswordprocessor	Atlantis Word Processor	3.0.2.5	All	All	All

cpe:2.3:a:atlantiswordprocessor:atlantis_word_processor:3.0.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:atlantiswordprocessor:atlantis_word_processor:3.0.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:atlantiswordprocessor:atlantis_word_processor:3.0.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:atlantiswordprocessor:atlantis_word_processor:3.0.2.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→