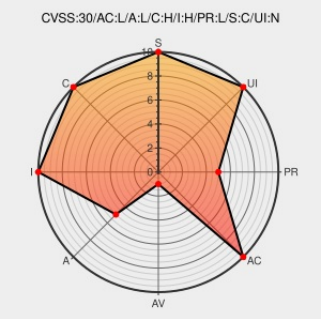
CVE-2018-18406

Published on: 06/19/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:53 PM UTC

CVE-2018-18406

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



Certain versions of Securetrack from Tufin contain the following vulnerability:

An issue was discovered in Tufin SecureTrack 18.1 with TufinOS 2.16 build 1179(Final). The Audit Report module is affected by a blind XXE vulnerability when a new Best Practices Report is saved using a special payload inside the xml input field. The XXE vulnerability is blind since the response doesn't directly display a requested file, but rather returns it inside the name data field when the report is saved. An attacker is able to view restricted operating system files. This issue affects all types of users: administrators or normal users.

CVE-2018-18406 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.9 - CRITICAL

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Network Security Policy Management, Firewall Management | Tufin	Vendor Advisory www.tufin.com text/html	MISC www.tufin.com/
TufinOS 2.17 Build 1193 - XML External Entity Injection - Linux webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	MISC www.exploit-db.com/exploits/45808
No Description Provided	Vendor Advisory forum.tufin.com text/html	MISC forum.tufin.com/support/kc/latest/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tufin	Securetrack	18.1	All	All	All
Application	Tufin	Securetrack	18.1	All	All	All
Operating System	Tufin	Tufinos	2.16	build_1179	All	All
Operating System	Tufin	Tufinos	2.16	build_1179	All	All

cpe:2.3:a:tufin:securetrack:18.1:*:*:*:*:*:*:*:

cpe:2.3:a:tufin:securetrack:18.1:*:*:*:*:*:*:*:

cpe:2.3:o:tufin:tufinos:2.16:build_1179:*:*:*:*:*:*:

cpe:2.3:o:tufin:tufinos:2.16:build_1179:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report