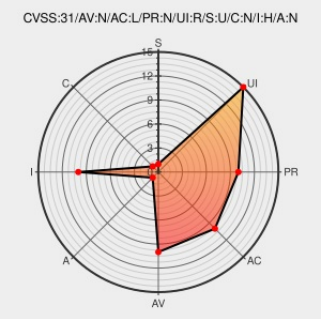
CVE-2019-9597

Published on: 10/23/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2019-9597

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



Certain versions of Enterprise Immune System from Darktrace contain the following vulnerability:

Darktrace Enterprise Immune System before 3.1 allows CSRF via the /config endpoint.

CVE-2019-9597 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2019-9596-and-CVE-2019-9597/poc.html at master · gerwout/CVE-2019-9596-and-CVE-2019-9597 · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/gerwout/CVE-2019-9596-and-CVE-2019-9597/blob/master/poc.html

Bugtraq: CSRF in Darktrace Enterprise Immune System <=3.0.10	Exploit Mailing List Third Party Advisory seclists.org text/html	BUGTRAQ 20190521 CSRF in Darktrace Enterprise Immune System <=3.0.10
Darktrace Enterpise Immune System 3.0.9 / 3.0.10 Cross Site Request Forgery ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/152986/Darktrace-Enterpise-Immune-System-3.0.9-3.0.10-Cross-Site-Request-Forgery.html
Peerlyst	Exploit Technical Description Third Party Advisory www.peerlyst.com text/html	MISC www.peerlyst.com/posts/exploiting-two-zero-days-in-a-darktrace-appliance-cve-2019-9596-and-cve-2019-9597-gerwout-van-der-veen

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Darktrace CSRF exploit

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Darktrace	Enterprise Immune System	All	All	All	All
Application	Darktrace	Enterprise Immune System	All	All	All	All

cpe:2.3:a:darktrace:enterprise_immune_system:*:*:*:*:*:*:*:*:

cpe:2.3:a:darktrace:enterprise_immune_system:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→