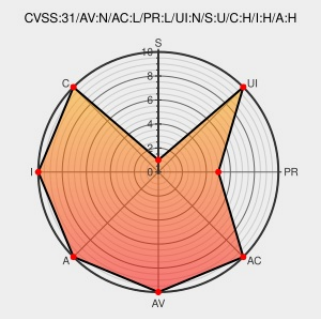
CVE-2021-36981

Published on: 08/30/2021 12:00:00 AM UTC

Last Modified on: 02/23/2023 02:57:00 AM UTC

CVE-2021-36981

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



Certain versions of Verinice from Sernet contain the following vulnerability:

In the server in SerNet verinice before 1.22.2, insecure Java deserialization allows remote authenticated attackers to execute arbitrary code.

CVE-2021-36981 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9 - HIGH

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

CVE References

Description	Tags	Link
Security Advisory	verinice.com text/html	MISC verinice.com/en/support/security-advisory
Comparing 1.22.1...1.22.2 · SerNet/verinice · GitHub	github.com text/html	MISC github.com/SerNet/verinice/compare/1.22.1...1.22.2

CVE-2021-36981 - Verinice.Pro 1.22.1 Unsafe Java deserialization of untrusted data, leading to remote code execution (authenticated) | SECIANUS	www.secianus.de text/html	MISC www.secianus.de/worum-geht-es/aktuelle-meldung/cve-2021-36981-verinicepro-unsafe-java-deserialization
GitHub - 0xBrAinsTorM/CVE-2021-36981	github.com text/html	MISC github.com/0xBrAinsTorM/CVE-2021-36981

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	Sernet	Verinice	All	All	All	All

cpe:2.3:a:sernet:verinice:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-36981 : In the server in SerNet verinice before 1.22.2, insecure Java deserialization allows remote authen… twitter.com/i/web/status/1…	2021-08-31 04:04:43
@threatmeter	CVE-2021-36981 In the server in SerNet verinice before 1.22.2, insecure Java deserialization allows remote authenti… twitter.com/i/web/status/1…	2021-09-01 07:11:13

← Previous ID

Next ID→