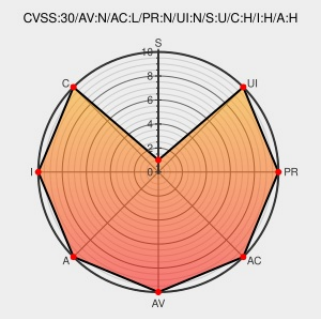
CVE-2018-1000854

Published on: 12/20/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:31 PM UTC

CVE-2018-1000854

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



Certain versions of Esigate from Esigate contain the following vulnerability:

esigate.org esigate version 5.2 and earlier contains a CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in ESI directive with user specified XSLT that can result in Remote Code Execution. This attack appear to be exploitable via Use of another weakness in backend application to reflect ESI directives. This vulnerability appears to have been fixed in 5.3.

CVE-2018-1000854 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Injection in XSLT parser : switch to secure mode · Issue #200	Third Party Advisory	MISC

Injection in XSLT parser : switch to secure mode · Issue #209 · esigate/esigate · GitHub	Third Party Advisory github.com text/html	MISC github.com/esigate/esigate/issues/209

Related QID Numbers

981039 Java (maven) Security Update for org.esigate:esigate-core (GHSA-hjm9-576q-399p)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Esigate	Esigate	All	All	All	All

cpe:2.3:a:esigate:esigate:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→