

CVE-2019-7609

Elastic Kibana Arbitrary Code Execution

Exigent

CISA KEV since Jan 10, 2022

Actively exploited

Public exploit module (Metasploit)

Kibana versions before 5.6.15 and 6.6.1 contain an arbitrary code execution flaw in the Timelion visualizer. An attacker with access to the Timelion application could send a request that will attempt to execute javascript code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.

EVRS 86/100 Immediate priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.953 99.87th percentile · FIRST	CISA DEADLINE Jul 10, 2022 KEV since 2022 · listed over a year
--	---	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.953 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
kibana	< 5.6.15 ≥ 6.0.0 < 6.6.1	5.6.15 · 6.6.1	NVD
openshift container platform	3.11 4.1	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-cp8f-5jp9-rqmh

NVD nvd.nist.gov/vuln/detail/CVE-2019-7609

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-17147

Additional guidance discuss.elastic.co/t/elastic-stack-6-6-1-and-5-6-15-security-update/169077

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2019-7609

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.