SOFTWARE VULNERABILITY RESEARCH DATASHEET

Delivering the world's best vulnerability intelligence

Software Vulnerability Research provides:

- Timeliness of vulnerability information being published
- Completeness of vulnerability information
- Accuracy of vulnerability information
- Actionability of advisories
- Risk context and information

Software Vulnerability Research summary

Flexera Software Vulnerability Research (SVR) provides access to verified intelligence from Secunia Research, the most reliable resource delivering the world's best software vulnerability intelligence, covering all applications and systems across all platforms. Prioritization is driven by threat intelligence, workflows, tickets and alerts, and describes the steps to mitigate the risk of costly breaches. So you stay in control.

Timeliness

Generally, **95 percent of incoming information about valid vulnerabilities that would result in a Secunia Advisory will be published within one business day. (A Secunia Advisory is an outline produced and published by our independent Secunia Research team describing what to expect when dealing with software vulnerabilities.)**

The other 5 percent? At times there is contradicting information from vendors, or missing information that requires a follow-up, which adds time to ensuring a complete and reliable advisory output.

- Even if a common vulnerabilities and exposure (CVE) identifier gets published by the vendor, the information updated to MITRE may be delayed. The National Vulnerability Database (NVD) can react only after the information gets updated on MITRE, while Secunia Research can react immediately once valid vulnerability information is public (regardless of source). Many vendors don't make publishing on MITRE a high priority, resulting in crucial delays.

Completeness

As of April 2020, SVR has 87,113 advisories covering 50,302 products across 10,978 vendors.

- SVR is the most robust software vulnerability database commercially available
- Secunia Research doesn't rely on CVE identifiers and the availability of information on MITRE like NVD does (NVD can act only if CVE entries get published on MITRE) and so we publish valid vulnerabilities without CVE identifiers (not all vulnerabilities get CVE identifiers), and such vulnerabilities without CVE identifiers never get published on NVD
- Customers can request products and version branches to be tracked, if we don't do so already

Accuracy (analysis process)

Data is received on both push and pull grounds from numerous sources (web, mailing lists, githubs, Microsoft API, etc.) providing vendor information and third-party information (like CERTs, packetstorm, exploit-db, etc.). This information is then classified concerning trustworthiness: specifically, vendor-related information is generally considered trusted, and certain CERTs (ICS-CERT, CERT/CC, AUScert, JVN) are generally semi-trusted. Regardless of trustworthiness, Secunia Research still analyzes the information presented regarding completeness and discrepancies.

If a source is untrusted, we'll confirm the potential vulnerability in a secure test environment (provided we have legal access to the product and are legally allowed to perform a vulnerability-related test) or we'll inquire through the vendor/maintainer if they'll acknowledge the potential vulnerability and can provide further information.

Our own analysis frequently includes development of our own proof of concept (POC) or at least the refinement of existing POCs to ensure, for example, that potential attacker control over the program workflow can be determined (DoS versus code execution, for instance).

All related, gathered information (trusted, semi-trusted, untrusted) is then aggregated and analyzed together. From there, we develop our own Secunia Research CVSSv3 metric and score while taking product context and security best practices into account. Product context is an important aspect as, for example, the exploitation and the impact of a valid vulnerability as reported in a library (OpenSSL) compared to a product implementing the library (for example, industrial control system) and exposing the same vulnerable functionality can differ significantly. If they do, we provide the differing outcome through the Secunia Advisory. NVD doesn't have any such product context available, so no matter what product is affected concerning a specific CVE identifier, NVD provides the very same rating. This allows a customer to compare Secunia Advisories regardless of who provides the source data.

The Secunia Research criticality rating is especially useful for prioritization as the usage of CVSSv3 frequently lets vulnerabilities end up in the upper brackets of the CVSSv3 scoring, which is not helpful. Our own criticality rating uses the whole scale from "not critical" through "extremely critical."

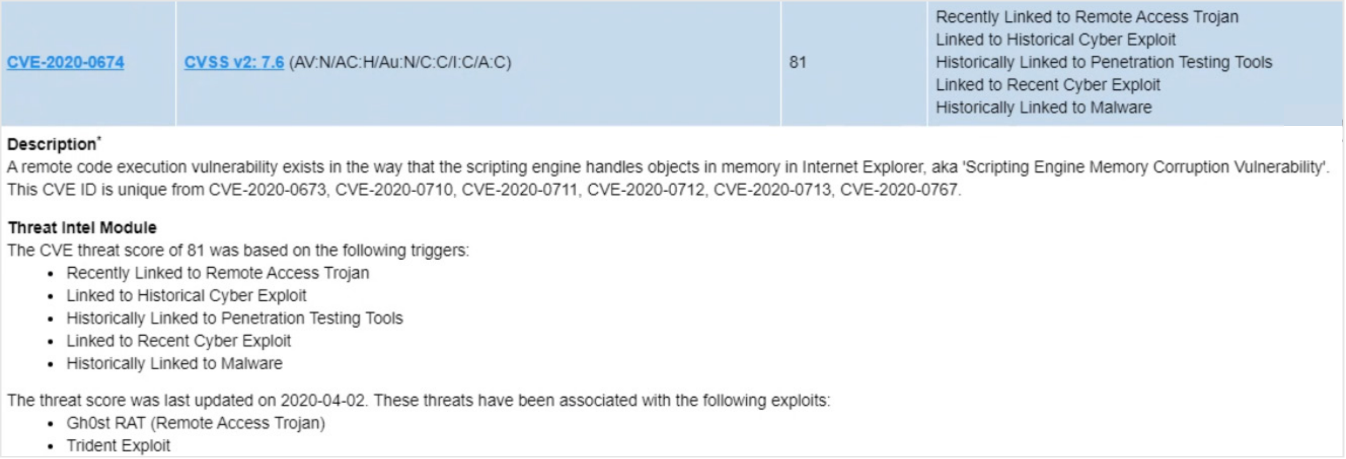
Actionability

Often, CVEs within the NVD don't contain details on the vulnerability but are in fact placeholders to be updated later. Secunia Advisories compile all CVEs applicable to a specific product version and provide details to the sum of the data into one advisory output, streamlining the process to triage the vulnerability information prior to distributing it to the appropriate teams.

- Customers can also alter the math within any ticket generated to better reflect their environment, a functionality lacking with CVEs via NVD
- Any information that may not be known when the advisory is published will be updated in the advisory and noted in its changelog

Risk context and information

Unlike public sources, Secunia Research provides associations of known exploits to the CVEs within an advisory for a product. The threat scores are set by severity of the threat posed quantified into categories of severity.



CVE-2020-0674	CVSS v2: 7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)	81	Recently Linked to Remote Access Trojan Linked to Historical Cyber Exploit Historically Linked to Penetration Testing Tools Linked to Recent Cyber Exploit Historically Linked to Malware

Description*
A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.

Threat Intel Module
The CVE threat score of 81 was based on the following triggers:

- Recently Linked to Remote Access Trojan
- Linked to Historical Cyber Exploit
- Historically Linked to Penetration Testing Tools
- Linked to Recent Cyber Exploit
- Historically Linked to Malware

The threat score was last updated on 2020-04-02. These threats have been associated with the following exploits:

- Gh0st RAT (Remote Access Trojan)
- Trident Exploit

Secunia Research enhanced CVE with Threat Intelligence

For more on how Software Vulnerability Research can help, visit our website

LEARN MORE

ABOUT FLEXERA

Flexera helps business leaders succeed at what once seemed impossible: getting full visibility into, and control of, their company's technology "black hole." From on-premises to the cloud, Flexera helps organizations unravel IT complexity and maximize business value from their technology investments. For more than 30 years, our 1300+ team members worldwide have been passionate about helping our more than 50,000 customers optimize IT to achieve their business outcomes. To learn more, visit **flexera.com**

1-800-374-4353 | +44 870-871-1111 | FLEXERA.COM

Flexera
Inform IT. Transform IT.™