SYNOPSYS®

GUIDE

Demonstrating the Value of Black Duck Security Advisories

Overview

Black Duck Security Advisories (BDSAs) are detailed open source vulnerability records sourced, curated, and analyzed by the Synopsys Cybersecurity Research Center (CyRC). BDSAs deliver timely, thorough, and actionable vulnerability research directly to Black Duck customer bills of materials (BOMs) so users can effectively prioritize and remediate vulnerabilities before a potential breach occurs.

In comparison, the Common Vulnerabilities and Exposures (CVE) list provides a reference method for publicly known cyber security vulnerabilities. A CVE entry contains an identification number (CVE ID), description, and public reference. Many entities around the world integrate CVEs into their products and services. The National Vulnerability Database (NVD) is the U.S. government repository of this vulnerability data.

4 factors for earlier, more actionable vulnerability information

Developers face a never-ending stream of vulnerability alerts that require their attention. So the earlier and more comprehensive and actionable the vulnerability information is, the easier it is for them to find and fix vulnerabilities and move on. Overall, BDSAs offer earlier notification and more complete, actionable open source vulnerability alerts compared to initial CVE entries and subsequent NVD research, as highlighted across four main categories:

- **Timing.** On average, a complete BDSA is published 14 days ahead of the corresponding researched CVE entry in the NVD.
- **Scoring.** In addition to Common Vulnerability Scoring System (CVSS) base scores, BDSAs include a temporal score, which refines the base score to provide more accurate severity metrics.
- **Detailed remediation guidance.** BDSAs include both clear and detailed remediation guidance and workaround options when available. And because Black Duck knows the context of your project, it also provides short- and long-term upgrade recommendations that are project-aware.
- **Completeness.** BDSAs provide a detailed title, a clear and concise summary of the vulnerability, and an extensive technical description. In addition, they provide the most relevant public references, including advisories, vendor upgrades, patch info, direct links to published exploits, and a timeline of key events.

Security vulnerability terms explained

Common Vulnerabilities and Exposures (CVE) is a dictionary that provides an identifier and description for publicly known cyber security vulnerabilities. The CVE allows organizations to identify vulnerabilities and share related data across tools, databases, and services, including the NVD.

The **Common Vulnerability Scoring System (CVSS)** is a framework for capturing the principal characteristics of a vulnerability to produce a numerical score that reflects its severity. CVSS scores consist of three core metric groups: base, temporal, and environmental.

- **Base scores** represent intrinsic qualities of a vulnerability and remain constant over time and across user environments. These scores are made of two subscores: exploitability and impact. Exploitability metrics look at attack vectors and complexity, or how attackers could execute an exploit and how easily they could do so. Impact metrics look at the potential impact of an exploit, or what attackers could gain access to (e.g., sensitive data) or disrupt (e.g., the availability of the application).
- **Temporal scores** adjust the base severity based on factors that change over time owing to events external to the vulnerability, such as the availability of an exploit, whether the report is confirmed, and what type of fix is available.
- **Environmental scores** adjust the base and temporal scores depending on a specific user environment. For example, environmental scores take into consideration the importance of the affected IT asset to a user's organization.

Common Weakness Enumeration (CWE) is a list of software and hardware weaknesses that have security ramifications. In terms of open source vulnerabilities, a CWE tells the developer what type of software weakness led to the vulnerability. A few common examples of CWEs are buffer overflow, SQL injection, denial of service, and cross-site scripting.

The **Synopsys Cybersecurity Research Center (CyRC)** works to accelerate access to information about software vulnerabilities, including identification, severity, exploitation, mitigation, and defense. CyRC's expertise spans static code

analysis, fuzzing, penetration testing, open source development, and production deployment. The open source vulnerability research team in Belfast, Northern Ireland, prioritizes their research based on issues that most affect Synopsys customers. The team is charged with identifying and researching open source software vulnerabilities, regardless of their report status in other security feeds or whether there is an associated CVE ID. The result of this research is presented to Black Duck customers in the form of a BDSA, offering quicker disclosure, complete remediation guidance, and detail and accuracy that the CVE lacks.

Apache Struts vulnerability example

Apache Struts, a popular open source framework for creating web applications, is widely used by Fortune 100 companies and others to build corporate websites. On March 8, 2017, the U.S. Department of Homeland Security sent out a notice addressing the need to patch an open source vulnerability in some versions of Apache Struts. The now-infamous vulnerability, CVE-2017-5638, had been publicly disclosed one day earlier.

Over the ensuing days and weeks, several development organizations became aware of this vulnerability, whether through the U.S. government notice, their manual monitoring of security feeds, or their use of a software composition analysis (SCA) tool, which monitors an open source BOM for new and existing open source vulnerabilities. Many organizations were able to patch the vulnerability before any data breach occurred. However, one very notable data breach gave hackers access to the sensitive data of millions of consumers.

We'll use this example to highlight the value of a BDSA record in quickly prioritizing and remediating a major open source vulnerability and compare it to the data provided by the NVD. Let's discuss how the four factors for timely and actionable vulnerability information described earlier apply to CVE-2017-5638.

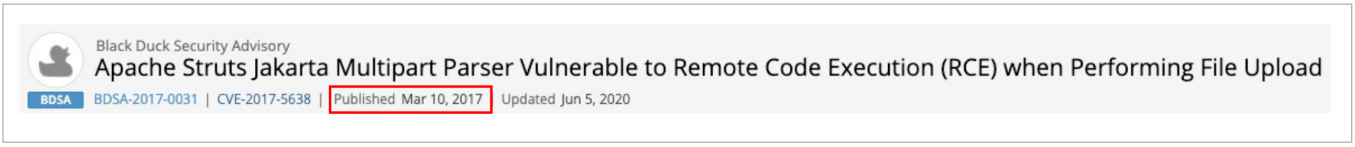
Timing

The public disclosure for CVE-2017-5638 was published on March 7, 2017, and a patch was available at that time. As stated, the U.S. Department of Homeland Security sent out its notice on March 8, 2017. Both contained a minimal amount of information and referenced the initial CVE information only.

The vulnerability was reported as BDSA-2017-0031 by the CyRC team on March 10, 2017, with descriptions, fixes, and references. The NVD also reported CVE-2017-5638 on March 10, 2017, but only as a placeholder with no real actionable information or research. At this point, the NVD entry included only the initial information available in the CVE record, a brief description, and a few unlabeled references, including a link to the patch. It wasn't until four days later, on March 14, 2017, that the NVD published its initial analysis, which included scoring, a link to the patch, the CWE, and labeled references.

It's important to note that the exploit was made public on March 5, 2017, so those first few days were critical. From the time an exploit is made public, the race is on between you and hackers, and you can win only with prompt notification and complete information.

Black Duck Security Advisory



National Vulnerability Database

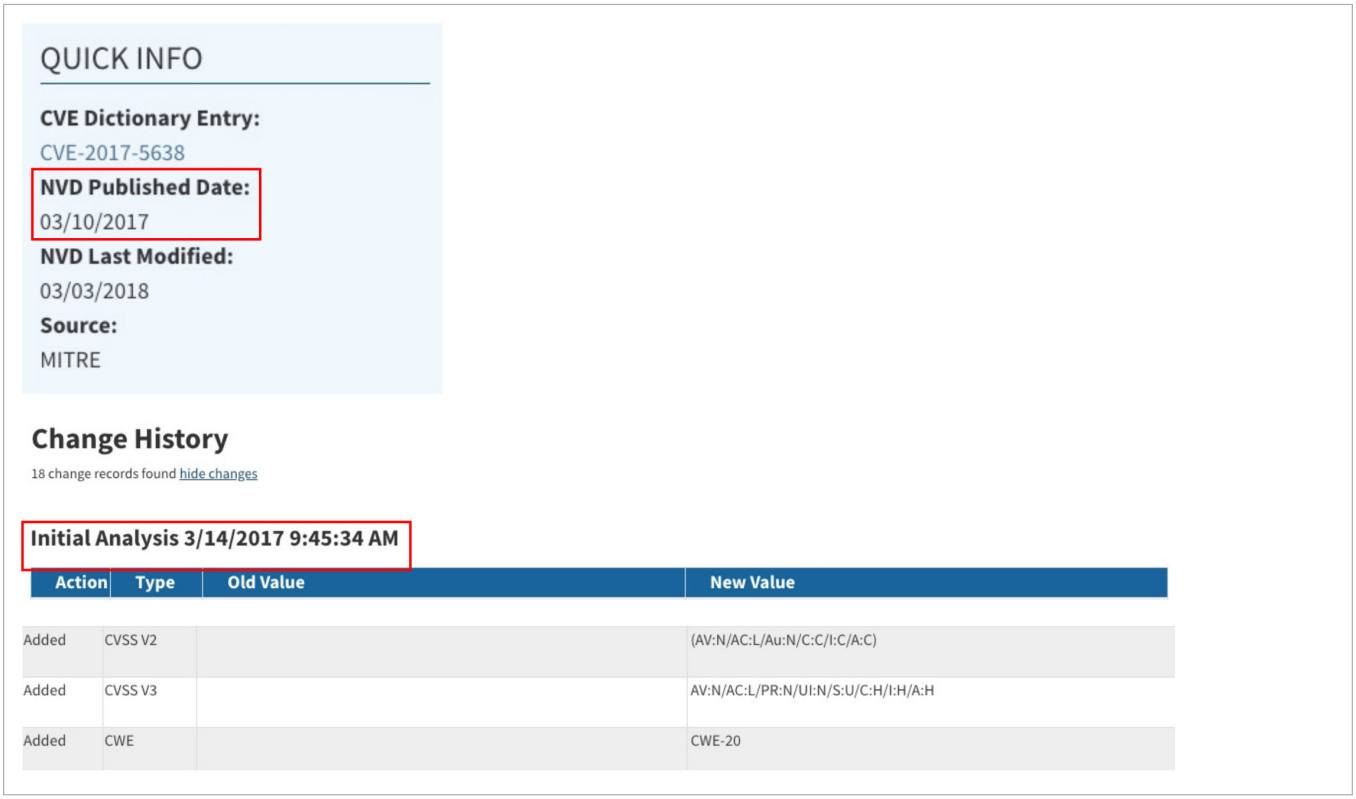
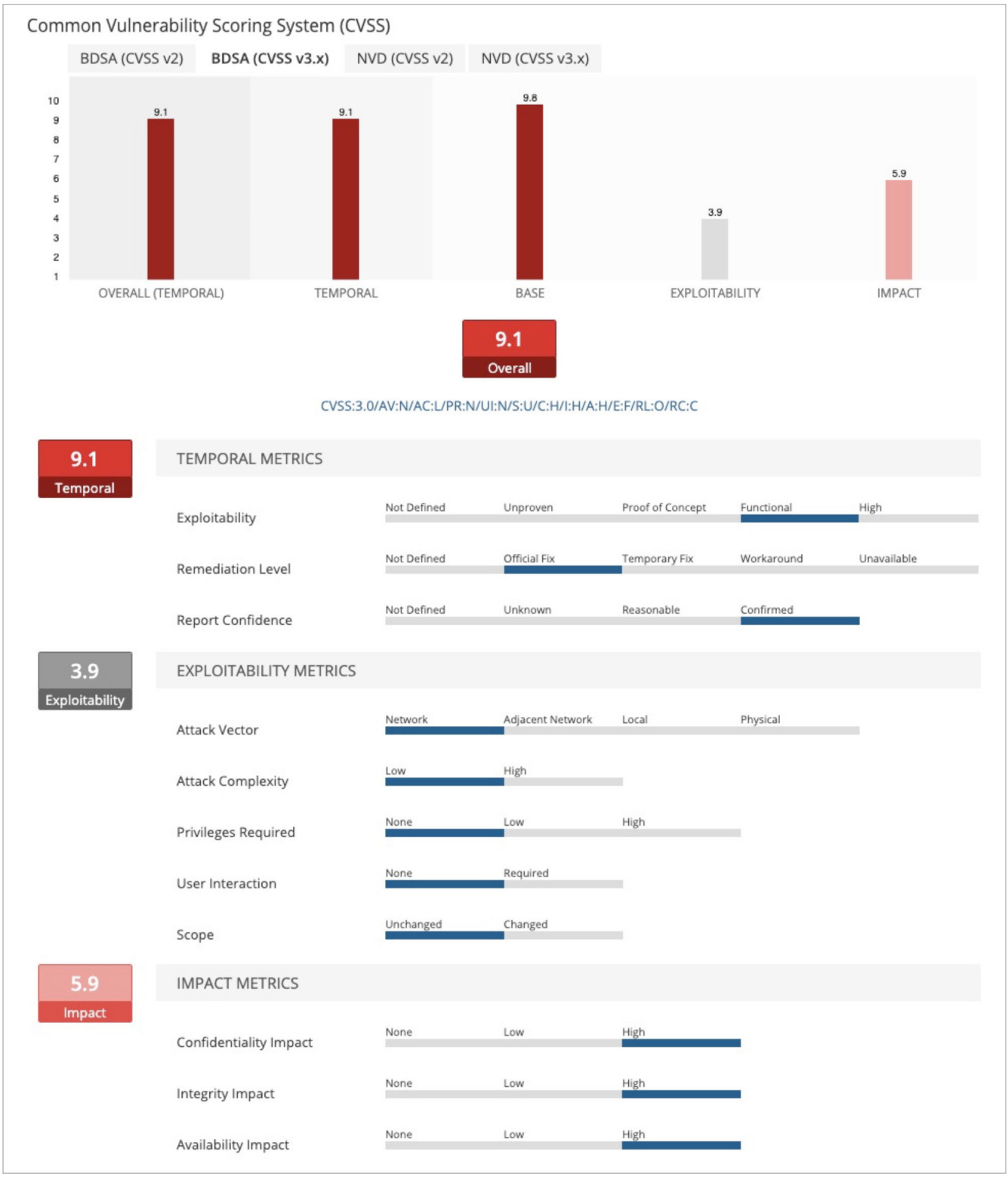


Figure 1: Timing

Scoring

The NVD reports an overall and base score of 10 for CVE-2017-5638. However, the BDSA for this vulnerability reports an overall score of 9.1. This score is still critical but tempered slightly from the NVD score because an official fix is available. The BDSA can assign a more appropriate level of risk by considering temporal metrics in its score. For reference, the BDSA also provides the NVD scoring details and displays all scores in an easy-to-consume format.

Black Duck Security Advisory



National Vulnerability Database

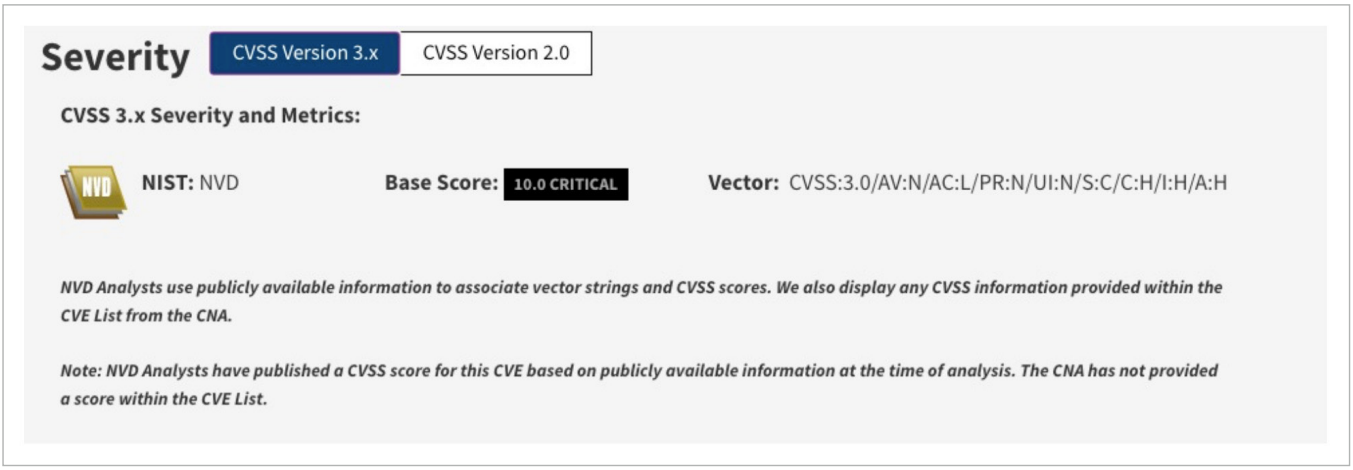


Figure 2: Scoring

Detailed remediation guidance

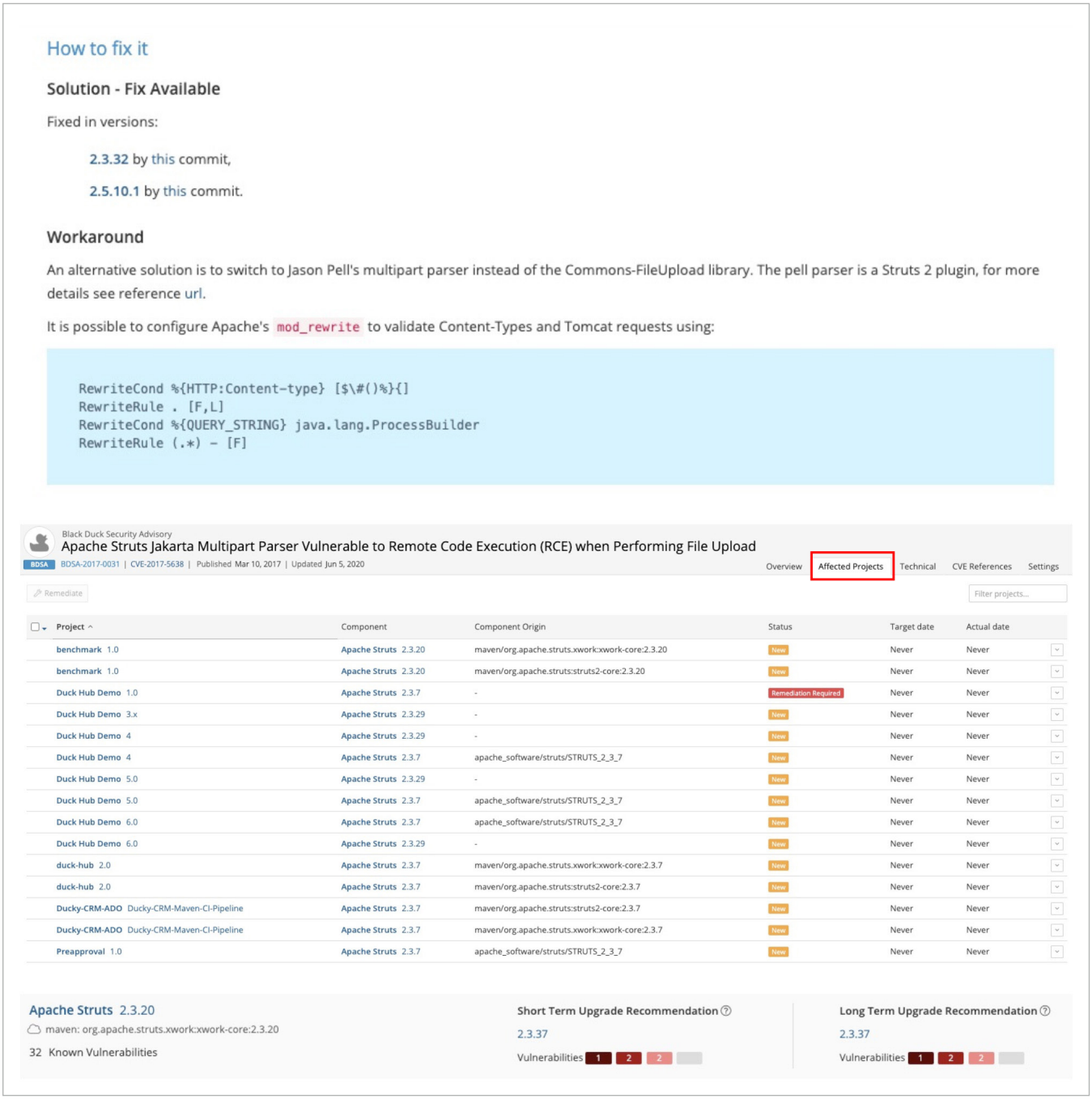
A BDSA takes three key factors into account when providing remediation guidance:

1. The BDSA points directly to the versions that fix the vulnerability and to the exact commit. If there are multiple ways to fix it, the BDSA points to each version and commit.
2. The CyRC team researches whether there is a viable workaround that doesn't require a full upgrade. If one exists, the BDSA provides detailed information on how to implement it.
3. Because Black Duck knows the context for your entire project, a BDSA provides both short- and long-term remediation guidance based on your current version and points you to any other projects that use the affected component. The short-term fix allows you to address the vulnerability (with fewer and less critical other issues) while remaining in your major version. The long-term upgrade recommendation brings you to the next nonvulnerable major version if one exists.

The BDSA for the Apache Struts vulnerability provides two remediation paths vetted and verified by CyRC: specific links to fixed versions of the component (e.g., version 2.3.32) and a comprehensive workaround for those unable to upgrade immediately.

In comparison, the NVD provides a long list of links to third-party references, including third-party advisories with technical descriptions, press coverage, vendor advisories, and available patches. Users have to sift through these links, find the patch info, and retrieve the solution appropriate for their environments. The NVD doesn't provide workaround information, and because it lacks context, it can't point users to the least disruptive fix for their environments or alert them to other projects containing the affected component.

Black Duck Security Advisory



How to fix it

Solution - Fix Available

Fixed in versions:

- 2.3.32 by this commit,
- 2.5.10.1 by this commit.

Workaround

An alternative solution is to switch to Jason Pell's multipart parser instead of the Commons-FileUpload library. The pell parser is a Struts 2 plugin, for more details see reference url.

It is possible to configure Apache's `mod_rewrite` to validate Content-Types and Tomcat requests using:

```
RewriteCond %{HTTP:Content-type} [$\#()%}{]
RewriteRule . [F,L]
RewriteCond %{QUERY_STRING} java.lang.ProcessBuilder
RewriteRule (.*) - [F]
```

Black Duck Security Advisory

Apache Struts Jakarta Multipart Parser Vulnerable to Remote Code Execution (RCE) when Performing File Upload

BDSA BDSA-2017-0031 | CVE-2017-5638 | Published Mar 10, 2017 | Updated Jun 5, 2020

Overview | Affected Projects | Technical | CVE References | Settings

Remediate | Filter projects...

Project	Component	Component Origin	Status	Target date	Actual date
benchmark 1.0	Apache Struts 2.3.20	maven/org.apache.struts.xwork:xwork-core:2.3.20	New	Never	Never
benchmark 1.0	Apache Struts 2.3.20	maven/org.apache.struts:struts2-core:2.3.20	New	Never	Never
Duck Hub Demo 1.0	Apache Struts 2.3.7	-	Remediation Required	Never	Never
Duck Hub Demo 3.x	Apache Struts 2.3.29	-	New	Never	Never
Duck Hub Demo 4	Apache Struts 2.3.29	-	New	Never	Never
Duck Hub Demo 4	Apache Struts 2.3.7	apache_software/struts/STRUTS_2_3_7	New	Never	Never
Duck Hub Demo 5.0	Apache Struts 2.3.29	-	New	Never	Never
Duck Hub Demo 5.0	Apache Struts 2.3.7	apache_software/struts/STRUTS_2_3_7	New	Never	Never
Duck Hub Demo 6.0	Apache Struts 2.3.7	apache_software/struts/STRUTS_2_3_7	New	Never	Never
Duck Hub Demo 6.0	Apache Struts 2.3.29	-	New	Never	Never
duck-hub 2.0	Apache Struts 2.3.7	maven/org.apache.struts.xwork:xwork-core:2.3.7	New	Never	Never
duck-hub 2.0	Apache Struts 2.3.7	maven/org.apache.struts:struts2-core:2.3.7	New	Never	Never
Ducky-CRM-ADO Ducky-CRM-Maven-CI-Pipeline	Apache Struts 2.3.7	maven/org.apache.struts:struts2-core:2.3.7	New	Never	Never
Ducky-CRM-ADO Ducky-CRM-Maven-CI-Pipeline	Apache Struts 2.3.7	maven/org.apache.struts.xwork:xwork-core:2.3.7	New	Never	Never
Preapproval 1.0	Apache Struts 2.3.7	apache_software/struts/STRUTS_2_3_7	New	Never	Never

Apache Struts 2.3.20

maven: org.apache.struts.xwork:xwork-core:2.3.20

32 Known Vulnerabilities

Short Term Upgrade Recommendation

2.3.37

Vulnerabilities 1 2 2

Long Term Upgrade Recommendation

2.3.37

Vulnerabilities 1 2 2

* Short- and long-term upgrade recommendations look at all vulnerabilities in the specific version of Apache Struts used in the project and provide recommendations based on that context.

National Vulnerability Database

Hyperlink	Resource
http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html	Technical Description, Third Party Advisory
http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/	Technical Description, Third Party Advisory
http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-002.txt	
http://www.eweek.com/security/apache-struts-vulnerability-under-attack.html	Press/Media Coverage
http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	
http://www.securityfocus.com/bid/96729	Third Party Advisory, VDB Entry
http://www.securitytracker.com/id/1037973	
https://arstechnica.com/security/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/	Press/Media Coverage
https://cwiki.apache.org/confluence/display/WW/S2-045	Mitigation, Vendor Advisory
https://cwiki.apache.org/confluence/display/WW/S2-046	
https://exploit-db.com/exploits/41570	Exploit, VDB Entry
https://git1-us-west.apache.org/repos/asf?p=struts.git;a=commit;h=352306493971e7d5a756d61780d57a76eb1f519a	Patch
https://git1-us-west.apache.org/repos/asf?p=struts.git;a=commit;h=6b8272ce47160036ed120a48345d9aa884477228	Patch
https://github.com/mazen160/struts-pwn	Exploit
https://github.com/rapid7/metasploit-framework/issues/8064	Exploit
https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03733en_us	
https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03749en_us	
https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03723en_us	
https://isc.sans.edu/diary/22169	Technical Description, Third Party Advisory
https://lists.apache.org/thread.html/r6d03e45b81eab03580cf7f8bb51cb3e9a1b10a2cc0c6a2d3cc92ed0c@%3Cannounce.apache.org%3E	
https://nmap.org/nsedoc/scripts/http-vuln-cve2017-5638.html	Third Party Advisory
https://packetstormsecurity.com/files/141494/S2-45-poc.py.txt	Exploit, VDB Entry
https://security.netapp.com/advisory/ntap-20170310-0001/	
https://struts.apache.org/docs/s2-045.html	
https://struts.apache.org/docs/s2-046.html	
https://support.lenovo.com/us/en/product_security/len-14200	
https://twitter.com/theog150/status/841146956135124993	Third Party Advisory
https://www.exploit-db.com/exploits/41614/	
https://www.imperva.com/blog/2017/03/cve-2017-5638-new-remote-code-execution-rce-vulnerability-in-apache-struts-2/	
https://www.kb.cert.org/vuls/id/834067	
https://www.symantec.com/security-center/network-protection-security-advisories/SA145	

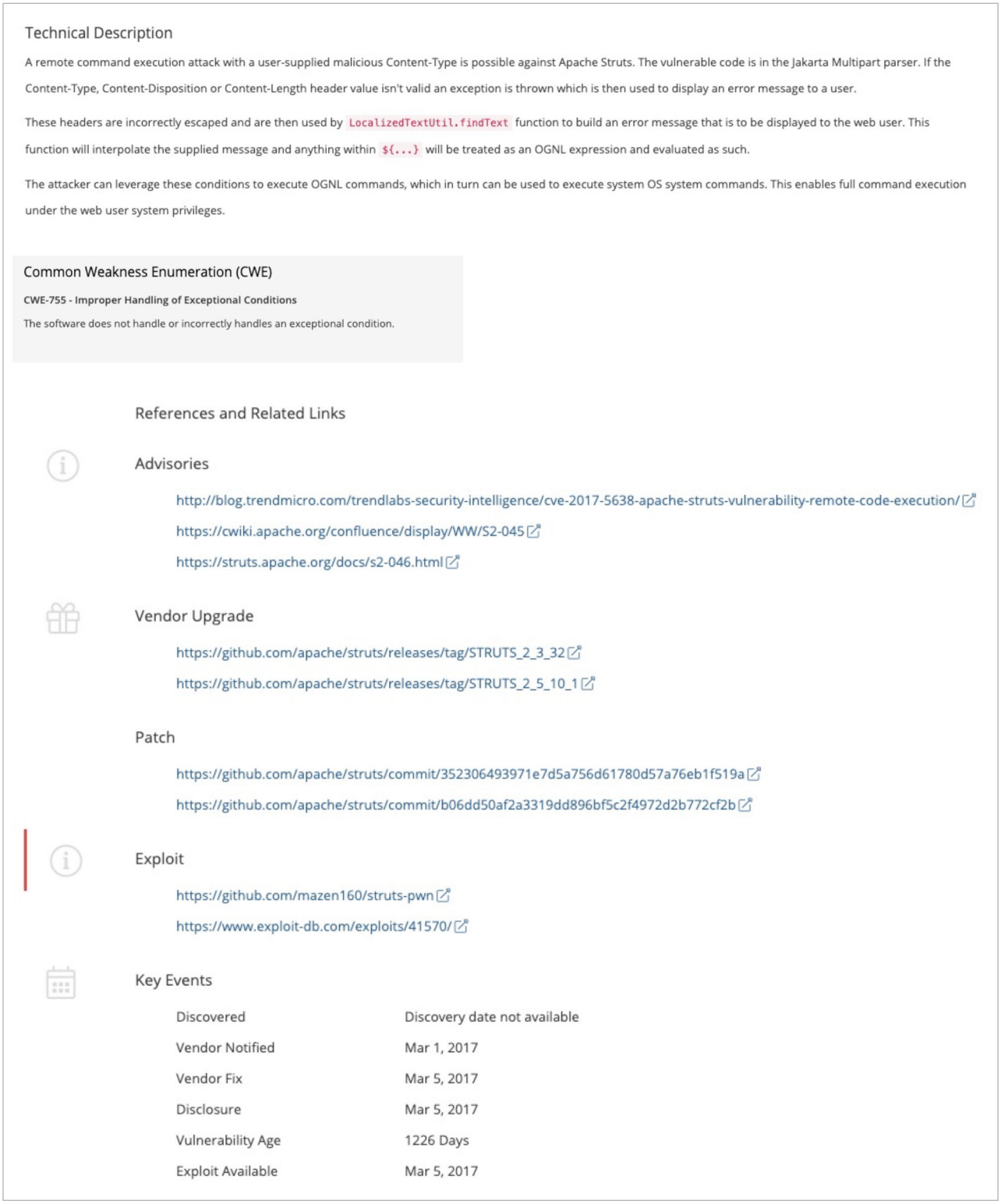
Figure 3: Detailed remediation guidance

Completeness

The BDSA for CVE-2017-5638 provides a full workup of the vulnerability, enabling users to assess, prioritize, and fix the vulnerability quickly. It provides a summary description and an in-depth technical description, links to multiple patches, a workaround (with code snippet), a detailed base and temporal score breakdown (side-by-side with those from the CVE) for more accurate prioritization, a description of the CWE that led to the vulnerability, a brief list of relevant references, exploit information, and a timeline of events so you can quickly understand the life of the vulnerability. For major vulnerable components such as Apache Struts (or for customer requests), the team also conducts in-depth analyses on vulnerabilities to identify the correct version ranges, test the exploits, and much more.

The NVD provides a baseline understanding of a vulnerability but lacks the critical information required to find and fix it quickly. The description is often unedited, contains heavy technical jargon, is difficult to understand, and doesn't include technical details. The scoring stops with the base score and doesn't assess temporal metrics, which are critical for understanding the true severity. The patch information and technical details are buried in a list of third-party links, without any potential workaround information or project-aware guidance.

Black Duck Security Advisory



National Vulnerability Database

Refer to Figure 3. Short- and long-term upgrade recommendations look at all vulnerabilities in the specific version of Apache Struts used in the project and provide recommendations based on that context.

Figure 4: Completeness

Conclusion

The National Vulnerability Database contains analyses on the thousands of CVE entries that are published to the CVE every year and serves as the U.S. government repository of this information. Development organizations that rely solely on this or similar sources often find themselves days behind and lacking the clear, complete, and actionable information required to find and fix open source vulnerabilities. Black Duck Security Advisories close these gaps and allow developers to use advanced research to automate the prioritization of critical open source vulnerabilities for fast and effective remediation.

Black Duck KnowledgeBase™ Facts

More than 249,000 unique vulnerabilities

Over 36,000 BDSAs providing more detail than NVD records

Over 3,500 Black Duck-exclusive vulnerabilities not found in the NVD

Published an average of 14 days ahead of the NVD

The Synopsys difference

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.