VASCO Security Advisory

Remote code execution vulnerability in Apache Struts 2 component in VASCO products

Advisory ID: vasco-sa-20170313-struts

Revision number: 1.2

Date and time of release: March 14 2017 8:00 UTC

Date and time of last update: March 17 2017 12:00 UTC

Summary

On Monday March 06, 2017 the Apache Struts 2 project issued a security bulletin about a Remote Code Execution vulnerability that exists in Apache Struts 2.

This security advisory contains information on the products that have been affected by the vulnerability and contains information on the availability of patches.

Impacted products

Following products are affected by the CVE-2017-5638 vulnerability:

- IDENTIKEY Authentication Server 3.5 and later
- IDENTIKEY Appliance 3.5.7.1 and later

Detailed description of vulnerability

The following vulnerability description is extracted from the NIST National Vulnerability Database:

“The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header, as exploited in the wild in March 2017.”

In scope of IDENTIKEY Authentication Server and IDENTIKEY Appliance, the vulnerability is present in the web administration component. The vulnerability can only be exploited by a malicious user if this user has access to web resources of the web administration component, such as for example the login page of the web administration component.

Severity score

The table below denotes the CVSS 2.0 vulnerability score of the CVE-2017-5638 vulnerability on VASCO's products.

CVSS Base Score: 6.8 (medium)					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Medium	None	Partial	Partial	Partial

Product fixes and workarounds

VASCO has released patches for the following products:

- IDENTIKEY Authentication Server 3.11/ IDENTIKEY Authentication Server 3.11 R2
- IDENTIKEY Authentication Server 3.10/ IDENTIKEY Authentication Server 3.10 R2
- IDENTIKEY Authentication Server 3.9
- IDENTIKEY Authentication Server 3.8
- IDENTIKEY Appliance 3.10.11.x
- IDENTIKEY Appliance 3.11.12.x

In order to limit the exploitability of the vulnerability, customers should limit the access to the IDENTIKEY web administration component as much as possible.

Obtaining product releases with fixes

Customers with a maintenance contract can obtain fixed product releases from the Customer Portal. Customers without a maintenance contract should contact their local sales representative.

References

[1] https://cwiki.apache.org/confluence/display/WW/S2-045
[2] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5638

Legal disclaimer

WHILE EVERY REASONABLE EFFORT IS MADE TO PROCESS AND PROVIDE INFORMATION THAT IS ACCURATE, ALL THE CONTENT AND INFORMATION IN THIS DOCUMENT ARE PROVIDED "AS IS" AND “AS AVAILABLE,” WITHOUT ANY REPRESENTATION OR ENDORSEMENT AND WITHOUT ANY EXPRESS OR IMPLIED GUARANTEE OF CURRENCY, COMPLETENESS OR SUITABILITY, OR ANY WARRANTY INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE OR PURPOSE. YOUR USE OF THIS DOCUMENT, ANY INFORMATION PROVIDED, OR OF MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK. VASCO RESERVES THE RIGHT TO CHANGE OR UPDATE THE INFORMATION IN THIS DOCUMENT AT ANY TIME AND AT ITS DISCRETION, AS AND WHEN NEW OR ADDITIONAL INFORMATION BECOMES AVAILABLE.