Micro Focus Security Update

UCMDB Browser

CVE-2017-5647, CVE-2017-5650, CVE-2017-5651 Multiple Apache Tomcat Vulnerabilities

Document management:

Date	Version	Change
September 18, 2017	Version 1.0	Initial release

Summary:

The following article enlists the necessary related details on the Micro Focus Product UCMDB Browser on the Apache Tomcat Vulnerabilities CVE-2017-5647, CVE-2017-5650, CVE-2017-5651.

Topic

CVE-2017-5647 A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

CVE-2017-5650 In Apache Tomcat 9.0.0.M1 to 9.0.0.M18 and 8.5.0 to 8.5.12, the handling of an HTTP/2 GOAWAY frame for a connection did not close streams associated with that connection that were currently waiting for a WINDOW_UPDATE before allowing the application to write more data. These waiting streams each consumed a thread. A malicious client could therefore construct a series of HTTP/2 requests that would consume all available processing threads.

CVE-2017-5651 In Apache Tomcat 9.0.0.M1 to 9.0.0.M18 and 8.5.0 to 8.5.12, the refactoring of the HTTP connectors introduced a regression in the send file processing. If the send file processing completed quickly, it was possible for the Processor to be added to the processor cache twice. This could result in the same Processor being used for multiple requests which in turn could lead to unexpected errors and/or response mix-up.

Reference's links (Nist if existing)

***Note**: This link provides further information about this issue and lists the Samba versions affected.*

Affected Releases: <Affected versions>

The following versions of UCMDB Browser for Universal CMDB were found vulnerable:

UCMDB Browser 4.10/4.11/4.12/4.13

Response

ACTION: Review all details in instructions provided in this paper to address the vulnerability.
Micro Focus recommend addressing this information as soon as possible.

Impact on UCMDB Browser

The UCMDB Browser for Universal CMDB is affected.

Mitigation Actions

Micro Focus has released the following software updates to resolve the vulnerability for the impacted versions of UCMDB Browser:

Note: Micro Focus recommends installing the latest software updates, if possible. Customers unable to apply the updates should contact Micro Focus Support to discuss options.

Affected versions	Solution	
UCMDB Browser 4.10/4.11/4.12/4.13	UCMDB Browser 4.14 **ITOM Marketplace**	