SSB-439005: Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP

Publication Date: 2018-11-27
Last Update: 2019-04-09
Current Version: V1.5

DESCRIPTION

Multiple vulnerabilities have been identified in the additional GNU/Linux subsystem of the current firmware version V2.6.0 for the SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP. These GNU/Linux vulnerabilities have been externally identified and will be fixed with the next firmware version.

Siemens is working on an update for the firmware, and recommends the following mitigations until an update is available:

- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security
- Only build and run applications from trusted sources

VULNERABILTY LIST

Relevant during runtime:

- CVE-2018-13053 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13053
- CVE-2018-14404 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14404
- CVE-2018-15473 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15473
- CVE-2018-17182 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17182
- CVE-2018-17972 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17972
- CVE-2018-19591 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19591
- CVE-2018-20784 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20784
- CVE-2019-7309 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7309
- CVE-2019-1559 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1559
- CVE-2019-9169 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9169

Relevant during buildtime:

- CVE-2018-6543 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6543
- CVE-2018-6759 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6759
- CVE-2018-6872 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6872
- CVE-2018-7208 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7208
- CVE-2018-7568 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7568
- CVE-2018-7569 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7569
- CVE-2018-7570 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7570
- CVE-2018-7642 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7642
- CVE-2018-7643 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7643
- CVE-2018-9138 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9138
- CVE-2018-9996 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9996
- CVE-2018-10534 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10534
- CVE-2018-10535 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10535
- CVE-2018-18605 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18605
- CVE-2018-18606 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18606
- CVE-2018-18607 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18607
- CVE-2018-18309 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18309
- CVE-2018-19931 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19931
- CVE-2018-19932 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19932
- CVE-2018-16862 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16862

- CVE-2018-20002 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20002
- CVE-2018-20623 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20623
- CVE-2018-20671 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20671
- CVE-2018-20651 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20651
- CVE-2018-1000876 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000876
- CVE-2019-6293 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6293
- CVE-2019-7146 - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-7146
- CVE-2019-7148 - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-7148
- CVE-2019-7149 - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-7149
- CVE-2019-7250 - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-7150
- CVE-2019-7664 - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-7664
- CVE-2019-7665 - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-7665

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2018-11-27):	Publication Date
V1.1 (2018-12-11):	Added CVE-2018-13053 and CVE-2018-19591
V1.2 (2019-01-08):	Added CVE-2018-19931 and CVE-2018-19932
V1.3 (2019-02-12):	Added CVE-2018-1000876 and CVE-2018-16862
V1.4 (2019-03-12):	Added CVE-2019-7309, CVE-2018-20002, CVE-2018-20671, CVE-2018-20651, CVE-2018-20623, CVE-2018-20784, CVE-2019-1559, CVE-2019-9169, CVE-2019-7146, CVE-2019-7148, CVE-2019-7149, CVE-2019-7150, CVE-2019-7664, CVE-2019-7665
V1.5 (2019-04-09):	Added CVE-2019-6293

TERMS OF USE

Siemens Security Bulletins are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.

