SIEMENS

ProductCERT Security Advisories

Siemens ProductCERT is the central team for responding to potential security incidents and vulnerabilities related to Siemens products, solutions and services. In the following, Siemens security advisories and bulletins issued by ProductCERT are listed.

2017

- SSA-151221 (Last Update 2017-02-13): Incorrect File Permissions in APOGEE Insight
- SSA-701708 (Last Update 2017-02-13): Local Privilege Escalation in Industrial Products
- SSA-931064 (Last Update 2017-02-13): Authentication Bypass in SIMATIC Logon

2016

- SSA-856492 (Last Update 2016-12-16): Limited Entropy in PRNG of Desigo PX Web Modules
- SSA-693129 (Last Update 2016-12-09): Vulnerability in SIMATIC WinCC and SIMATIC PCS 7
- SSA-731239 (Last Update 2016-12-09): Vulnerabilities in SIMATIC S7-300 and S7-400 CPUs
- SSA-946325 (Last Update 2016-11-25): Vulnerabilities in SICAM PAS
- SSA-603476 (Last Update 2016-11-21): Web Vulnerabilities in SIMATIC CP 343-1/CP 443-1 Modules and SIMATIC S7-300/S7-400 CPUs
- SSA-672373 (Last Update 2016-11-18): Vulnerabilities in SIMATIC CP 1543-1
- SSA-284765 (Last Update 2016-11-16): Vulnerability in SIEMENS-branded IP-based CCTV Cameras
- SSA-296574 (Last Update 2016-10-21): Denial of Service in SICAM RTU Devices
- SSA-869766 (Last Update 2016-10-12): Information Disclosure Vulnerabilities in SIMATIC STEP 7 (TIA Portal) V12 and V13
- SSA-284342 (Last Update 2016-10-12): Vulnerabilities in Automation License Manager (ALM)
- SSA-342135 (Last Update 2016-09-22): Web Vulnerability in SCALANCE M-800 / S615
- SSA-630413 (Last Update 2016-09-05): Vulnerabilities in SIPROTEC 4 and SIPROTEC Compact
- SSA-321174 (Last Update 2016-10-12): Privilege Escalation in SINEMA Server
- SSA-378531 (Last Update 2016-11-07): Vulnerabilities in SIMATIC WinCC, PCS 7 and WinCC Runtime Professional
- SSA-453276 (Last Update 2016-07-22): Denial-of-Service Vulnerability in SIMATIC NET PC-Software
- SSA-119132 (Last Update 2016-07-22): Cross-Site Scripting Vulnerability in SINEMA Remote Connect Server
- SSA-444217 (Last Update 2016-11-25): Information Disclosure Vulnerabilities in SICAM PAS
- SSA-526760 (Last Update 2016-06-08): Weak Credentials Protection in SIMATIC WinCC flexible
- SSA-818183 (Last Update 2016-06-08): Denial-of-Service Vulnerability in S7-300 CPU
- SSA-547990 (Last Update 2016-06-30): Information Disclosure Vulnerabilities in SIPROTEC 4 and SIPROTEC Compact
- SSA-751155 (Last Update 2016-04-08): Denial-of-Service Vulnerability in SCALANCE S613
- SSA-623229 (Last Update 2016-04-08): DROWN Vulnerability in Industrial Products
- SSA-301706 (Last Update 2016-09-22): GNU C Library Vulnerability in Industrial Products
- SSA-833048 (Last Update 2016-03-14): Vulnerability in SIMATIC S7-1200 CPUs prior to V4
- SSA-253230 (Last Update 2016-02-08): Vulnerabilities in SIMATIC S7-1500 CPU
- SSA-743465 (Last Update 2016-01-15): Cross-Site Scripting Vulnerability in OZW672 and OZW772

2015

- SSA-472334 (Last Update 2015-12-18): NTP Vulnerabilities in RUGGEDCOM ROX-based Devices
- SSA-763427 (Last Update 2016-04-29): Vulnerability in Communication Processor (CP) modules SIMATIC CP 343-1, TIM 3V-IE, TIM 4R-IE, and CP 443-1
- SSA-921524 (Last Update 2016-04-29): Incorrect Frame Padding in ROS-based Devices
- SSA-720081 (Last Update 2015-09-01): IP Forwarding in RUGGEDCOM ROS-based Devices
- SSA-134003 (Last Update 2015-08-27): Web Vulnerability in S7-1200
- SSA-504631 (Last Update 2015-08-04): Incorrect Certificate Validation in COMPAS Mobile App
- SSA-267489 (Last Update 2015-07-21): Vulnerability in Android App Sm@rtClient
- SSA-396873 (Last Update 2015-12-18): TLS Vulnerability in Ruggedcom ROS- and ROX-based Devices
- SSA-732541 (Last Update 2015-07-17): Denial-of-Service Vulnerability in SIPROTEC 4
- SSA-632547 (Last Update 2015-07-14): Authentication Bypass Vulnerability in SICAM MIC
- SSA-142512 (Last Update 2015-06-25): Cross-Site Scripting Vulnerability in Climatix BACnet/IP Communication Module
- SSA-311412 (Last Update 2015-05-04): Incorrect Certificate Verification in Android App HomeControl for Room Automation

- SSA-237894 (Last Update 2015-09-28): Vulnerability in SIMATIC PCS 7
- SSA-487246 (Last Update 2015-08-27): Vulnerabilities in SIMATIC HMI Devices
- SSA-994726 (Last Update 2015-04-22): GHOST Vulnerability in Siemens Industrial Products
- SSA-335471 (Last Update 2015-03-05): Denial-of-Service Vulnerability in SPC Controller Series
- SSA-451236 (Last Update 2015-04-22): Vulnerability in SIMATIC ProSave, SIMATIC CFC, SIMATIC STEP 7, SIMOTION Scout, and STARTER
- SSA-987029 (Last Update 2015-03-05): Denial-of-Service Vulnerability in S7-300
- SSA-185226 (Last Update 2015-03-05): Vulnerabilities in App SPCanywhere
- SSA-749212 (Last Update 2015-03-05): NTP Vulnerabilities in SINUMERIK Controllers
- SSA-315836 (Last Update 2015-08-27): Vulnerabilities in SIMATIC STEP 7 (TIA Portal) V12 and V13
- SSA-543623 (Last Update 2015-02-13): Vulnerabilities in SIMATIC WinCC (TIA Portal) V13
- SSA-234789 (Last Update 2015-02-13): Vulnerabilities in SIMATIC STEP 7 (TIA Portal) V13
- SSA-753139 (Last Update 2015-02-03): Vulnerabilities in Ruggedcom WIN Products
- SSA-954136 (Last Update 2015-02-02): User Impersonation Vulnerability in SCALANCE X-200IRT Switch Family
- SSA-597212 (Last Update 2015-01-21): Web Vulnerability in SIMATIC S7-1200
- SSA-321046 (Last Update 2015-01-19): Denial-of-Service Vulnerabilities in SCALANCE X-300/X408 Switch Family
- SSA-671683 (Last Update 2015-03-05): NTP Vulnerabilities in Ruggedcom ROX-based Devices
- SSA-311299 (Last Update 2015-01-13): Vulnerabilities in iOS App SIMATIC WinCC Sm@rtClient

2014

- SSA-134508 (Last Update 2015-02-06): Vulnerabilities in SIMATIC WinCC, PCS 7 and WinCC in TIA Portal
- SSB-583110 (Last update 2014-11-10): Customer Information about POODLE Attack on SSLv3 Protocol Vulnerabilities
- SSA-860967 (Last Update 2015-02-13): GNU Bash Vulnerabilities in Siemens Industrial Products
- SSA-310688 (Last Update 2014-08-14): Denial-of-Service Vulnerability in SIMATIC S7-1500 CPU
- SSA-214365 (Last Update 2014-10-07): Vulnerabilities in SIMATIC WinCC
- SSA-234763 (Last Update 2015-02-13): OpenSSL Vulnerabilities in Siemens Industrial Products
- SSA-839231 (Last Update 2014-10-16): Incorrect Certificate Verification in Ruggedcom ROX-based Devices
- SSA-892012 (Last Update 2014-04-24): Web Vulnerabilities in SIMATIC S7-1200 CPU
- SSA-635659 (Last Update 2014-08-14): Heartbleed Vulnerability in Siemens Industrial Products
- SSA-364879 (Last Update 2014-04-15): Vulnerabilities in SINEMA Server
- SSA-353456 (Last Update 2014-04-08): BEAST Attack Vulnerability in Ruggedcom WIN Products
- SSA-831997 (Last Update 2014-12-15): Denial-of-Service Vulnerability in Ruggedcom ROS-based Devices
- SSA-654382 (Last Update 2014-04-15): Vulnerabilities in SIMATIC S7-1200 CPU
- SSA-724606 (Last Update 2014-03-20): Denial-of-Service Vulnerabilities in SIMATIC S7-1200 PLCs
- SSA-456423 (Last Update 2014-03-12): Vulnerabilities in SIMATIC S7-1500 CPU
- SSA-892342 (Last Update 2014-05-23): Denial-of-Service Vulnerability in RuggedCom ROS-based Devices
- SSA-342587 (Last Update 2014-03-20): Vulnerabilities in SIMATIC WinCC Open Architecture

2013

- SSA-568732 (Last Update 2013-12-13): Privilege Escalation in COMOS
- SSA-324789 (Last Update 2013-12-06): Vulnerabilities in RuggedCom ROS-based Devices
- SSA-742938 (Last Update 2013-12-17): Open Ports in SINAMICS S/G Firmware
- SSA-176087 (Last Update 2013-10-18): Unauthenticated Access to Critical Services in SCALANCE X-200 Switch Family
- SSA-850708 (Last Update 2013-10-18): Authentication Bypass in SCALANCE X-200 Switch Family
- SSA-970879 (Last Update 2013-12-17): Privilege Escalation in COMOS
- SSA-120908 (Last Update 2013-07-31): Vulnerabilities in Siemens Scalance W-7xx (a/b/g) Product Family
- SSA-064884 (Last Update 2013-07-31): Vulnerabilities in WinCC (TIA Portal)
- SSA-345843 (Last Update 2013-06-24): Vulnerabilities in WinCC 7.2
- SSA-194865 (Last Update 2013-06-20): Security Vulnerability in Siemens COMOS
- SSA-170686 (Last Update 2013-05-27): Vulnerabilities in Siemens Scalance X200 IRT Switch Family
- SSA-212483 (Last Update 2013-03-15): Vulnerabilities in WinCC (TIA Portal) V11
- SSA-714398 (Last Update 2013-03-22): Vulnerabilities in WinCC 7.0 SP3 Update 1
- SSA-628113 (Last Update 2013-02-18): Open Debugging Port in CP 1616 and CP 1604
- SSA-963338 (Last Update 2014-06-13): Multiple Buffer Overflows in UPnP Interface of OZW and OZS Products
- SSA-099471 (Last Update 2013-01-14): Buffer overflow in Simatic RF Manager

2012

- SSA-783261 (Last Update 2012-12-12): Denial-of-Service vulnerability in Siemens Automation License Manager (ALM)
- SSA-370812 (Last Update 2013-01-22): Insecure Password Storage in Siemens ProcessSuite (discontinued product)
- SSA-938777 (Last Update 2012-10-08): Possible Remote Code Execution in SiPass Integrated

- SSA-279823 (Last Update 2012-10-08): Cross-Site Scripting Vulnerability in the SIMATIC S7-1200 Web Application
- SSA-240718 (Last Update 2012-09-13) Insecure storage of HTTPS CA certificate in S7-1200 V2.x
- SSA-864051 (Last Update 2012-09-10) Multiple Vulnerabilities in WinCC 7.0 SP3
- SSA-622607 (Last Update 2012-12-12) RuggedCom Private Key Vulnerabilities for HTTPS/SSL and SSH
- SSA-312568 (Last Update 2012-08-10): Security Vulnerability in COMOS
- SSA-617264 (Last Update 2012-07-30): Security Vulnerability in SIMATIC S7-400 V5 PN CPUs
- SSA-589272 (Last Update 2012-07-30): Security Vulnerability in SIMATIC S7-400 V6 PN CPUs
- SSA-283911 (Last Update 2012-07-30): Security Vulnerability in Synco OZW Devices
- SSA-110665 (Last Update 2012-10-19): Security Vulnerability in SIMATIC STEP7
- SSA-027884 (Last Update 2012-07-23): Security Vulnerability in SIMATIC WinCC
- SSA-826381 (Last Update 2012-06-14): Multiple Security Vulnerabilities in RuggedCom ROS-based Devices
- SSA-223158 (Last Update 2012-06-05): Multiple Security Vulnerabilities in WinCC 7.0 SP3
- SSA-268149 (Last Update 2012-04-05): Multiple Security Vulnerabilities in Siemens Scalance S
- SSA-130874 (Last Update 2012-04-05): Multiple Security Vulnerabilities in Siemens Scalance X Switches
- SSA-345442 (Last update 2012-01-26): Multiple Vulnerabilities in WinCC flexible and WinCC V11 (TIA Portal)
- SSA-850510 (Last update 2012-01-19): Siemens Tecnomatix FactoryLink Multiple ActiveX Vulnerabilities

2011

- SSA-319258 (Last Update 2011-12-16): Multiple Security Vulnerabilities in Siemens Automation License Manager (ALM)
- SSA-625789 (Last Update 2011-09-12): Security Vulnerabilities in Siemens SIMATIC S7-1200 CPU
- SSA-460621 (Last Update 2011-09-05) :Security Vulnerability in Siemens WinCC Flexible Runtime Loader Could Allow Memory Corruption
- SSA-191374 (Last Update 2011-05-27): Vulnerability in ActiveReports component of WinCC flexible/RF Manager Could Allow Code Execution
- SSA-170396 (Last Update 2011-05-20): Vulnerability in Tag Simulator for WinCC flexible Could Allow Code Execution
- SSA-630126 (Last Update 2011-03-30): Multiple Vulnerabilities in Siemens Tecnomatix Factory

A description of our vulnerability handling guidelines and policies can be found here.

If you would like to report a vulnerability or security issues relating to Siemens products or solutions, please contact

✉ productcert@siemens.com

- Only emails composed in English or German can be considered
- Checked 7 days a week, response within one work day

The following public PGP key is available for encrypted communication:

- PGP

Key fingerprint: 1C36 704D 88D7 0A12 00B3 1A56 6E75 3C94 F2EB CF9C

In case of other general IT security issues relating to Siemens, please contact:

✉ cert@siemens.com

Related Links

- German CERT-Association (in German)
- Forum of Incident Response and Security Teams
- International Information Integrity Institute
- Corporate CERT Services (Intranet)
- ANSSI Recommendations on Cybersecurity for ICS (in English and French)

Downloads

- Vulnerability Handling

Contact

- productcert@siemens.com

- Follow us on Twitter

siemens.com Global Website |