SSA-451445: Multiple Vulnerabilities in SPPA-T3000

Publication Date: 2019-12-10
Last Update: 2022-02-17
Current Version: V1.2
CVSS v3.1 Base Score: 9.8

SUMMARY

SPPA-T3000 Application Server and MS3000 Migration Server are affected by multiple vulnerabilities. Some of the vulnerabilities can allow an attacker to execute arbitrary code on the server. Exploitation of the vulnerabilities described in this advisory requires access to either Application- or Automation Highway. Both highways should not be exposed if the environment has been set up according to the recommended system configuration in the SPPA-T3000 security manual.

In this case Siemens Energy considers the environmental score as CR:L/IR:L/AR:H/MAV:A for vulnerabilities related to the Application Server and CR:L/IR:L/AR:M/MAV:A for vulnerabilities related to the Migration Server.

Siemens Energy provides a service pack to fix vulnerabilities on the Application Server and recommends configurations to mitigate the vulnerabilities in the Migration Server. Detailed information will be available for SPPA-T3000 customers in the Siemens Energy Customer Portal (https://cep.siemens-energy.com/).

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SPPA-T3000 Application Server: All versions < Service Pack R8.2 SP2 only affected by CVE-2018-4832, CVE-2019-18283, CVE-2019-18284, CVE-2019-18285, CVE-2019-18286, CVE-2019-18287, CVE-2019-18288, CVE-2019-18314, CVE-2019-18315, CVE-2019-18316, CVE-2019-18317, CVE-2019-18318, CVE-2019-18319, CVE-2019-18320, CVE-2019-18331, CVE-2019-18332, CVE-2019-18333, CVE-2019-18334, CVE-2019-18335	Please contact your Siemens Energy service management organization to obtain the update to Service Pack R8.2 SP2. See further recommendations from section Workarounds and Mitigations
SPPA-T3000 MS3000 Migration Server: All versions only affected by CVE-2019-18289, CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18293, CVE-2019-18294, CVE-2019-18295, CVE-2019-18296, CVE-2019-18297, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, CVE-2019-18307, CVE-2019-18308, CVE-2019-18309, CVE-2019-18310, CVE-2019-18311, CVE-2019-18312, CVE-2019-18313, CVE-2019-18321, CVE-2019-18322, CVE-2019-18323, CVE-2019-18324, CVE-2019-18325, CVE-2019-18326, CVE-2019-18327, CVE-2019-18328, CVE-2019-18329, CVE-2019-18330	Apply released configuration specifications for SPPA-T3000 MS3000 available with Service Pack R8.2 SP2 to mitigate these vulnerabilities. See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Implement mitigations described in the SPPA-T3000 security manual
- Restrict access to the Application Highway using the SPPA-T3000 Firewall
- External components should be connected only to the SPPA-T3000 DMZ; no bridging of an external network to either the Application- or Automation highways is allowed
- Perform regular updates of the SPPA-T3000 (e.g. by using the Security Server if available)
- Implement mitigations provided in the customer information letter distributed via the customer service portal
- Please contact your local Siemens Energy representative if you need help at securing your SPPA-T3000 installation

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design.

Siemens Energy strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens Energy strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure Siemens Energy strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

SPPA-T3000 is a distributed control system mostly used in fossil and large scale renewable power plants.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2018-4832

Specially crafted messages sent to the RPC service of the affected products could cause a Denial-of-Service condition on the remote and local communication functionality of the affected products. A reboot of the system is required to recover the remote and local communication functionality.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2019-18283

The AdminService is available without authentication on the Application Server. An attacker can gain remote code execution by sending specifically crafted objects to one of its functions.

Please note that an attacker needs to have access to the Application Highway in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-502: Deserialization of Untrusted Data

Vulnerability CVE-2019-18284

The AdminService is available without authentication on the Application Server. An attacker can use methods exposed via this interface to receive password hashes of other users and to change user passwords.

Please note that an attacker needs to have access to the Application Highway in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18285

The RMI communication between the client and the Application Server is unencrypted. An attacker with access to the communication channel can read credentials of a valid user.

Please note that an attacker needs to have access to the Application Highway in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-319: Cleartext Transmission of Sensitive Information

Vulnerability CVE-2019-18286

The Application Server exposes directory listings and files containing sensitive information.

This vulnerability is independent from CVE-2019-18287.

Please note that an attacker needs to have access to the Application Highway in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18287

The Application Server exposes directory listings and files containing sensitive information.

This vulnerability is independent from CVE-2019-18286.

Please note that an attacker needs to have access to the Application Highway in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18288

An attacker with valid authentication at the RMI interface could be able to gain remote code execution through an unsecured file upload.

Please note that an attacker needs to have access to the Application Highway in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-434: Unrestricted Upload of File with Dangerous Type

Vulnerability CVE-2019-18289

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18293, CVE-2019-18295, and CVE-2019-18296.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18290

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18291

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18292

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18293

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18289, CVE-2019-18295, and CVE-2019-18296.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18294

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18295

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18289, CVE-2019-18293, and CVE-2019-18296.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18296

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18289, CVE-2019-18293, and CVE-2019-18295.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18297

An attacker with local access to the MS3000 Server and low privileges could gain root privileges by sending specifically crafted packets to a named pipe.

Please note that an attacker needs to have local access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18298

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-18299

An attacker with network access to the MS3000 Server can trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-18300

An attacker with network access to the MS3000 Server can trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-18301

An attacker with network access to the MS3000 Server can trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-18302

An attacker with network access to the MS3000 Server can trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-18303

An attacker with network access to the MS3000 Server can trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-18304

An attacker with network access to the MS3000 Server can trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18305, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-18305

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18306, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-18306

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, and CVE-2019-18307.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2019-18307

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, and CVE-2019-18306.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:U/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2019-18308

An attacker with local access to the MS3000 Server and a low privileged user account could gain root privileges by manipulating specific files in the local file system.

This vulnerability is independent from CVE-2019-18309.

Please note that an attacker needs to have local access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2019-18309

An attacker with local access to the MS3000 Server and a low privileged user account could gain root privileges by manipulating specific files in the local file system.

This vulnerability is independent from CVE-2019-18308.

Please note that an attacker needs to have local access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2019-18310

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition by sending specifically crafted packets to port 7061/tcp.

This vulnerability is independent from CVE-2019-18311.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2019-18311

An attacker with network access to the MS3000 Server could trigger a Denial-of-Service condition by sending specifically crafted packets to port 7061/tcp.

This vulnerability is independent from CVE-2019-18310.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-952: SFP Secondary Cluster: Missing Authentication

Vulnerability CVE-2019-18312

An attacker with network access to the MS3000 Server could be able to enumerate running RPC services.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18313

An attacker with network access to the MS3000 Server could gain remote code execution by sending specifically crafted objects to one of the RPC services.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-434: Unrestricted Upload of File with Dangerous Type

Vulnerability CVE-2019-18314

An attacker with network access to the Application Server could gain remote code execution by sending specifically crafted objects via RMI.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18315

An attacker with network access to the Application Server could gain remote code execution by sending specifically crafted packets to 8888/tcp.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18316

An attacker with network access to the Application Server could gain remote code execution by sending specifically crafted packets to 1099/tcp.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-502: Deserialization of Untrusted Data

Vulnerability CVE-2019-18317

An attacker with network access to the Application Server could cause a Denial-of-Service condition by sending specifically crafted objects via RMI.

This vulnerability is independent from CVE-2019-18318 and CVE-2019-18319.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18318

An attacker with network access to the Application Server can cause a Denial-of-Service condition by sending specifically crafted objects via RMI.

This vulnerability is independent from CVE-2019-18317 and CVE-2019-18319.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18319

An attacker with network access to the Application Server could cause a Denial-of-Service condition by sending specifically crafted objects via RMI.

This vulnerability is independent from CVE-2019-18317 and CVE-2019-18318.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18320

An attacker with network access to the Application Server could be able to upload arbitrary files without authentication.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18321

An attacker with network access to the MS3000 Server could be able to read and write arbitrary files on the local file system by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18322.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18322

An attacker with network access to the MS3000 Server could be able to read and write arbitrary files on the local file system by sending specifically crafted packets to port 5010/tcp.

This vulnerability is independent from CVE-2019-18321.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18323

An attacker with network access to the MS3000 Server could cause a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to 5010/tcp.

This vulnerability is independent from CVE-2019-18324, CVE-2019-18325, CVE-2019-18326, CVE-2019-18327, CVE-2019-18328, CVE-2019-18329, and CVE-2019-18330.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18324

An attacker with network access to the MS3000 Server can cause a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to 5010/tcp.

This vulnerability is independent from CVE-2019-18323, CVE-2019-18325, CVE-2019-18326, CVE-2019-18327, CVE-2019-18328, CVE-2019-18329, and CVE-2019-18330.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18325

An attacker with network access to the MS3000 Server can cause a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to 5010/tcp.

This vulnerability is independent from CVE-2019-18323, CVE-2019-18324, CVE-2019-18326, CVE-2019-18327, CVE-2019-18328, CVE-2019-18329, and CVE-2019-18330.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18326

An attacker with network access to the MS3000 Server can cause a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to 5010/tcp.

This vulnerability is independent from CVE-2019-18323, CVE-2019-18324, CVE-2019-18325, CVE-2019-18327, CVE-2019-18328, CVE-2019-18329, and CVE-2019-18330.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18327

An attacker with network access to the MS3000 Server can cause a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to 5010/tcp.

This vulnerability is independent from CVE-2019-18323, CVE-2019-18324, CVE-2019-18325, CVE-2019-18326, CVE-2019-18328, CVE-2019-18329, and CVE-2019-18330.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18328

An attacker with network access to the MS3000 Server can cause a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to 5010/tcp.

This vulnerability is independent from CVE-2019-18323, CVE-2019-18324, CVE-2019-18325, CVE-2019-18326, CVE-2019-18327, CVE-2019-18329, and CVE-2019-18330.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18329

An attacker with network access to the MS3000 Server can cause a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to 5010/tcp.

This vulnerability is independent from CVE-2019-18323, CVE-2019-18324, CVE-2019-18325, CVE-2019-18326, CVE-2019-18327, CVE-2019-18328, and CVE-2019-18330.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18330

An attacker with network access to the MS3000 Server could cause a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to 5010/tcp.

This vulnerability is independent from CVE-2019-18323, CVE-2019-18324, CVE-2019-18325, CVE-2019-18326, CVE-2019-18327, CVE-2019-18328, and CVE-2019-18329.

Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-18331

An attacker with network access to the Application Server could gain access to path and filenames on the server by sending specifically crafted packets to 1099/tcp.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2019-18332

An attacker with network access to the Application Server could gain access to directory listings of the server by sending specifically crafted packets to 80/tcp, 8095/tcp or 8080/tcp.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2019-18333

An attacker with network access to the Application Server could gain access to filenames on the server by sending specifically crafted packets to 8090/tcp.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2019-18334

An attacker with network access to the Application Server could be able to enumerate valid user names by sending specifically crafted packets to 8090/tcp.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2019-18335

An attacker with network access to the Application Server could be able to gain access to logs and configuration files by sending specifically crafted packets to 80/tcp.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Vyacheslav Moskvin and Ivan B from Positive Technologies for coordinated disclosure of CVE-2019-18314 to CVE-2019-18330
- Gleb Gritsai, Eugenie Potseluevskaya, Sergey Andreev, and Radu Motspan from Kaspersky Lab for coordinated disclosure of CVE-2018-4832 and CVE-2019-18283 to CVE-2019-18313
- Can Demirel from Biznet Bilişim for coordinated disclosure of CVE-2019-18331 to CVE-2019-18335

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 (2019-12-10): Publication Date
V1.1 (2020-03-10): Added updates and configuration recommendations
V1.2 (2022-02-17): Editorial changes, assigned to Siemens Energy

TERMS OF USE