Schneider Electric ETG3000 FactoryCast HMI Gateway Use of Hard-coded Credentials

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-9198
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-27 19:59:10 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The FTP server on the Schneider Electric ETG3000 FactoryCast HMI Gateway with firmware through 1.60 IR 04 has hardc

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-798 | CWE-255 | CWE-798 CWE-798

Version	Source	Type	Score	Severity	Vector
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C
2.0	ics-cert@hq.dhs.gov	Secondary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C
2.0	CNA	CVSS	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Schneider-electric	Etg3000 Factorycast Hmi Gateway Firmware	All	All	All	All
Hardware	Schneider-electric	Tsxetg3000	-	All	All	All
Hardware	Schneider-electric	Tsxetg3010	-	All	All	All
Hardware	Schneider-electric	Tsxetg3021	-	All	All	All
Hardware	Schneider-electric	Tsxetg3022	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Schneider Electric	ETG3000 FactoryCast HMI Gateway	affected TSXETG3000	Not specified
CNA	Schneider Electric	ETG3000 FactoryCast HMI Gateway	affected TSXETG3010	Not specified
CNA	Schneider Electric	ETG3000 FactoryCast HMI Gateway	affected TSXETG3021	Not specified
CNA	Schneider Electric	ETG3000 FactoryCast HMI Gateway	affected TSXETG3022	Not specified

References

Reference	Source	Li
Schneider Electric ETG3000 FactoryCast HMI Gateway Authentication Bypass Vulnerability	af854a3a-2127-422b-91ae-364da2661108	w
Schneider Electric ETG3000 FactoryCast HMI Gateway Vulnerabilities | ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	ics
www.cisa.gov/news-events/ics-advisories/icsa-15-020-02	ics-cert@hq.dhs.gov	w
RETIRED: Tsxetg3010 CVE-2014-9198 Remote Security Vulnerability	af854a3a-2127-422b-91ae-364da2661108	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

Vendor Comments And Credit

Discovery Credit

CNA: Narendra Shinde of Qualys Security (en)

Additional Advisory Data

Solutions

CNA: Schneider Electric has produced an updated firmware, labelled V1.60 IR 04. This firmware release moves the jar files directory in a secure area. The new firmware also includes the ability to disable the FTP server. This updated firmware can be downloaded at: http://www.schneider-electric.com/download/WW/EN/details/681790255-TSXETG30xx-V160-

IR4/?showAsIframe... http://www.schneider-electric.com/download/WW/EN/details/681790255-TSXETG30xx-V160-IR4/

Workarounds

CNA: Schneider Electric recommends the FTP server be deactivated when not needed. The firmware update does not remove the hard-coded credentials. Narendra Shinde also found that configuration files were accessible using default credentials. Schneider Electric recommends users change the default login credentials. This will protect configuration files from unauthorized access.

Legacy QID Mappings

590491 Schneider Electric ETG3000 FactoryCast HMI Gateway Multiple Vulnerabilities (ICSA-15-020-02)