Cyber Security Advisory #07/2020

Multiple Vulnerabilities in GateManager

Document Version: 1.0

First published: 2020-09-29
Last updated: N/A (Initial version)

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee.

B&R provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall B&R or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if B&R or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from B&R, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Executive Summary

CVE-2020-14500 GateManager Improper HTTP Request Handling Vulnerability
An improper HTTP request handling vulnerability in B&R GateManager 4260 and 9250 versions <9.0.20276 and GateManager 8250 versions <9.2.620276048 allows remote, unauthenticated users to overwrite arbitrary data and to perform remote code execution.

CVE-2020-14508 GateManager Off-By-One Error Vulnerability
An off-by-one error vulnerability in B&R GateManager 4260 and 9250 versions <9.0.20276 and GateManager 8250 versions <9.2.620276048 allows remote, unauthenticated users to impact availability and to perform remote code execution.

CVE-2020-14510 GateManager Default Telnet Credentials Vulnerability
A default Telnet credentials vulnerability in B&R GateManager 4260 and 9250 versions <9.0.20276 and GateManager 8250 versions <9.2.620276048 allows remote, authenticated users to execute commands as root.

CVE-2020-14512 GateManager Credential Storage Weakness Vulnerability
A credential storage weakness vulnerability in B&R GateManager 4260 and 9250 versions <9.0.20276 and GateManager 8250 versions <9.2.620276048 allows remote, authenticated users to obtain sensitive user account data.

Affected Products

Affected products: GateManager
Affected versions:

- GateManager 4260 and 9250 <v9.0.20276
- GateManager 8250 <v9.2.620276048

The following versions are **not affected:**

- GateManager 4260 and 9250 v9.0.20276 and higher
- GateManager 8250 v9.2. 620276048 and higher

Vulnerability ID

CVE-2020-14500 GateManager Improper HTTP Request Handling Vulnerability
CVE-2020-14508 GateManager Off-By-One Error Vulnerability
CVE-2020-14510 GateManager Default Telnet Credentials Vulnerability
CVE-2020-14512 GateManager Credential Storage Weakness Vulnerability

Vulnerability Severity

The severity assessment is based on the FIRST Common Vulnerability Scoring System (CVSS) v3.1.

CVE-2020-14500	GateManager Improper HTTP Request Handling Vulnerability
CVSS v3.1 Base Score:	10.0 (Critical)
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE-2020-14508	GateManager Off-By-One Error Vulnerability
CVSS v3.1 Base Score:	8.1 (High)
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2020-14510	GateManager Default Telnet Credentials Vulnerability
CVSS v3.1 Base Score:	9.8 (Critical)
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2020-14512	GateManager Credential Storage Weakness Vulnerability
CVSS v3.1 Base Score:	9.1 (Critical)
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Corrective Actions or Resolution

The described vulnerabilities have been fixed in the following product versions:

- GateManager 4260 and 9250 v9.0.20276
- GateManager 8250 v9.2. 620276048

Vulnerability Details

CVE-2020-14500 GateManager Improper HTTP Request Handling Vulnerability

Description

When processing HTTP headers, the GateManager HTTP request handler applies a subset of input validation only. Upon receipt of specially crafted HTTP requests, the request handler performs an out-of-bounds write operation.

Impact

An unauthenticated adversary can overwrite arbitrary data, potentially leading to remote code execution on vulnerable GateManager instances.

Fix

The HTTP request handler now fully validates the HTTP header field in question.

Workarounds and Mitigations

B&R has not identified any specific workarounds or mitigations for this vulnerability.
Security solutions like Intrusion Prevention Systems and Web Application Firewalls may be able to prevent exploitation of this vulnerability by blocking exploit traffic before it reaches GateManager instances. Further details are provided in our Cyber Security guidelines – see section "Supporting information and guidelines" below.

CVE-2020-14508 GateManager Off-By-One Error Vulnerability

Description

When processing HTTP requests with certain properties, a memory cleanup bug is triggered in GateManager.

Impact

An unauthenticated adversary can crash the GateManager service, potentially leading to remote code execution on vulnerable GateManager instances.

Fix

The memory cleanup bug has been fixed.

Workarounds and Mitigations

B&R has not identified any specific workarounds or mitigations for this vulnerability.

CVE-2020-14510 GateManager Default Telnet Credentials Vulnerability

Description

The Telnet service includes a command execution feature intended for debug purposes only.

Impact

An authenticated adversary can run arbitrary commands with root privileges.

Fix

The command execution feature has been removed from the Telnet service.

Workarounds and Mitigations

B&R has not identified any specific workarounds or mitigations for this vulnerability.

CVE-2020-14512 GateManager Credential Storage Weakness Vulnerability

Description

GateManager lacks strong access control and strong encryption regarding stored credentials of privileged user accounts.

Impact

An authenticated adversary may be able to decrypt credentials of privileged user accounts stored on GateManager instances.

Fix

The credential storage weaknesses have been eliminated.

Workarounds and Mitigations

B&R has not identified any specific workarounds or mitigations for this vulnerability.

Supporting information and guidelines

The B&R Cyber Security webpage provides further information including Cyber Security guidelines. Please find these resources here: https://www.br-automation.com/en/service/cyber-security/

Acknowledgements

B&R would like to thank the following for working with us to help protect our customers:

- Sharon Brizinov and Tal Keren from Claroty

Document History

Version	Date	Description
1.0	2020-09-29	Initial version