Cyber Security Advisory #06/2020

Multiple Vulnerabilities in SiteManager and 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-2020-11641 SiteManager Local File Inclusion Vulnerability
A local file inclusion vulnerability in B&R SiteManager versions <9.2.620236042 allows authenticated users to read sensitive files from SiteManager instances.

CVE-2020-11642 SiteManager Denial of Service via Local File Inclusion Vulnerability
The local file inclusion vulnerability present in B&R SiteManager versions <9.2.620236042 allows authenticated users to impact availability of SiteManager instances.

CVE-2020-11643 GateManager Information Disclosure Vulnerability
An information disclosure vulnerability in B&R GateManager 4260 and 9250 versions <9.0.20262 and GateManager 8250 versions <9.2.620236042 allows authenticated users to view information of devices belonging to foreign domains.

CVE-2020-11644 GateManager Audit Message Spoofing Vulnerability
The information disclosure vulnerability present in B&R GateManager 4260 and 9250 versions <9.0.20262 and GateManager 8250 versions <9.2.620236042 allows authenticated users to generate fake audit log messages.

CVE-2020-11645 GateManager Denial of Service Vulnerability
A denial of service vulnerability in B&R GateManager 4260 and 9250 versions <9.0.20262 and GateManager 8250 versions <9.2.620236042 allows authenticated users to limit availability of GateManager instances.

CVE-2020-11646 GateManager Log Information Disclosure Vulnerability
A log information disclosure vulnerability in B&R GateManager 4260 and 9250 versions <9.0.20262 and GateManager 8250 versions <9.2.620236042 allows authenticated users to view log information reserved for other users.

Affected Products

Affected products: SiteManager and GateManager
Affected versions:

- Site Manager <v9.2.620236042
- GateManager 4260 and 9250 <v9.0.20262
- GateManager 8250 <v9.2.620236042

The following versions are **not affected:**

- SiteManager v9.2.620236042 and higher
- GateManager 4260 and 9250 v9.0.20262 and higher
- GateManager 8250 v9.2.620236042 and higher

Vulnerability ID

CVE-2020-11641 SiteManager Local File Inclusion Vulnerability
CVE-2020-11642 SiteManager Denial of Service via Local File Inclusion Vulnerability
CVE-2020-11643 GateManager Information Disclosure Vulnerability
CVE-2020-11644 GateManager Audit Message Spoofing Vulnerability
CVE-2020-11645 GateManager Denial of Service Vulnerability
CVE-2020-11646 GateManager Log Information Disclosure Vulnerability

Vulnerability Severity

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

CVE-2020-11641 SiteManager Local File Inclusion Vulnerability
CVSS v3.1 Base Score: 7.7 (High)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CVE-2020-11642 SiteManager Denial of Service via Local File Inclusion Vulnerability
CVSS v3.1 Base Score: 7.7 (High)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

CVE-2020-11643 GateManager Information Disclosure Vulnerability
CVSS v3.1 Base Score: 6.5 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVE-2020-11644 GateManager Audit Message Spoofing Vulnerability
CVSS v3.1 Base Score: 6.5 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

CVE-2020-11645 GateManager Denial of Service Vulnerability
CVSS v3.1 Base Score: 6.5 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVE-2020-11646 GateManager Log Information Disclosure Vulnerability
CVSS v3.1 Base Score: 4.3 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Corrective Actions or Resolution

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

- SiteManager v9.2.620236042
- GateManager 4260 and 9250 v9.0.20262
- GateManager 8250 v9.2.620236042

Vulnerability Details

CVE-2020-11641 SiteManager Local File Inclusion Vulnerability

Description

SiteManager contains a Web application powering the Web GUI used to manage a SiteManager instance. This Web application allows to read sensitive files located on a SiteManager instance.

Impact

An authenticated adversary can read service configuration and other sensitive information, potentially abusing this information for malicious activities on SiteManager instances.

Fix

The Web application now denies to read local files from a SiteManager instance.

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 SiteManager instances. Further details are provided in our Cyber Security guidelines – see section "Supporting information and guidelines" below.

CVE-2020-11642 SiteManager Denial of Service via Local File Inclusion Vulnerability

Description

Abusing the Local File Inclusion Vulnerability outlined above may cause SiteManager instances to restart.

Impact

An authenticated adversary can repeatedly trigger a restart of SiteManager instances, thus limiting their availability.

Fix

This vulnerability is a consequence of the Local File Inclusion Vulnerability - the fix for the Local File Inclusion Vulnerability also fixes this vulnerability.

Workarounds and Mitigations

This vulnerability is a consequence of the Local File Inclusion Vulnerability – please check the respective section of the parent vulnerability "CVE-2020-11641 SiteManager Local File Inclusion Vulnerability".

CVE-2020-11643 GateManager Information Disclosure Vulnerability

Description

On GateManager instances serving multiple, independent organizations, a vulnerability in the audit log feature allows cross-domain access to information of foreign devices.

Impact

An authenticated adversary can gather information about devices belonging to a foreign organization, potentially abusing this information for malicious activities.

Fix

The audit log code now prevents cross-domain access to device information.

Workarounds and Mitigations

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

CVE-2020-11644 GateManager Audit Message Spoofing Vulnerability

Description

A vulnerability in the GateManager audit log feature may be abused to generate fake audit messages/alerts.

Impact

An authenticated adversary can fool users of foreign domains with fictional audit messages/alerts of their choice.

Fix

The audit log code no longer allows a user to write fictional audit messages/alerts to the audit log.

Workarounds and Mitigations

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

CVE-2020-11645 GateManager Denial of Service Vulnerability

Description

A vulnerability in the GateManager Ping feature may cause a GateManager instance to restart.

Impact

An authenticated adversary can repeatedly trigger a restart of GateManager instances, thus limiting their availability.

Fix

The code of the Ping feature has been fixed, eliminating the potential to cause a GateManager restart.

Workarounds and Mitigations

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

CVE-2020-11646 GateManager Log Information Disclosure Vulnerability

Description

A vulnerability in the GateManager audit log feature may leak log information reserved for a specific user to other users.

Impact

An authenticated adversary can view information about all devices belonging to his/her domain, potentially abusing this information for malicious activities.

Fix

The code of the audit log feature no longer allows cross-user access to audit logs.

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:

- Nikolay Sokolik and Hay Mizrachi from Otorio

Document History

Version	Date	Description
1.0	2020-09-29	Initial version