Multiple vulnerabilities in BAT-C2

Date: 2022-11-23
Version: 1.0

Summary

The following vulnerabilities affect one or more versions of the products listed in the next section:

ID	Title / Description	Severity
CVE-2021-21872	An OS command injection vulnerability exists in the Web Manager Diagnostics: Traceroute functionality of Hirschmann BAT-C2. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.9
CVE-2021-21873	A specially-crafted HTTP request can lead to arbitrary command execution in RSA keypasswd parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.1
CVE-2021-21875	A specially-crafted HTTP request can lead to arbitrary command execution in EC keypasswd parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.1
CVE-2021-21876	Specially-crafted HTTP requests can lead to arbitrary command execution in PUT requests. An attacker can make authenticated HTTP requests to trigger this vulnerability.	CVSSv3.1: 9.1
CVE-2021-21877	Specially-crafted HTTP requests can lead to arbitrary command execution in “GET” requests. An attacker can make authenticated HTTP requests to trigger this vulnerability.	CVSSv3.1: 9.1
CVE-2021-21878	A local file inclusion vulnerability exists in the Web Manager Applications and FsBrowse functionality of Hirschmann BAT-C2. A specially-crafted series of HTTP requests can lead to local file inclusion. An attacker can make a series of authenticated HTTP requests to trigger this vulnerability.	CVSSv3.1: 4.9
CVE-2021-21879	A directory traversal vulnerability exists in the Web Manager File Upload functionality of Hirschmann BAT-C2. A specially-crafted HTTP request can lead to arbitrary file overwrite. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 8.8
CVE-2021-21880	A directory traversal vulnerability exists in the Web Manager FsCopyFile functionality of Hirschmann BAT-C2. A specially-crafted HTTP request can lead to local file inclusion. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 7.2
CVE-2021-21881	An OS command injection vulnerability exists in the Web Manager Wireless Network Scanner functionality of Hirschmann BAT-C2. A specially-crafted HTTP request can lead to command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.9
CVE-2021-21882	An OS command injection vulnerability exists in the Web Manager FsUnmount functionality of Hirschmann BAT-C2. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 8.8
CVE-2021-21883	An OS command injection vulnerability exists in the Web Manager Diagnostics: Ping functionality of	CVSSv3.1: 9.9

	Hirschmann BAT-C2. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	
CVE-2021-21884	An OS command injection vulnerability exists in the Web Manager SslGenerateCSR functionality of Hirschmann BAT-C2. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.1
CVE-2021-21885	A directory traversal vulnerability exists in the Web Manager FsMove functionality of Hirschmann BAT-C2. A specially crafted HTTP request can lead to local file inclusion. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 7.2
CVE-2021-21886	A directory traversal vulnerability exists in the Web Manager FSBrowsePage functionality of Hirschmann BAT-C2. A specially crafted HTTP request can lead to information disclosure. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 4.3
CVE-2021-21887	A stack-based buffer overflow vulnerability exists in the Web Manager SslGenerateCSR functionality of Hirschmann BAT-C2. A specially crafted HTTP request can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.1
CVE-2021-21888	An OS command injection vulnerability exists in the Web Manager SslGenerateCertificate functionality of Hirschmann BAT-C2. A specially crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.1
CVE-2021-21889	A stack-based buffer overflow vulnerability exists in the Web Manager Ping functionality of Hirschmann BAT-C2 specially crafted HTTP request can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.9
CVE-2021-21890	A stack-based buffer overflow vulnerability exists in the Web Manager FsBrowseClean functionality of Hirschmann BAT-C2. A specially crafted HTTP request can lead to remote code execution in the vulnerable portion of the branch (deletedir). An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.1
CVE-2021-21891	A stack-based buffer overflow vulnerability exists in the Web Manager FsBrowseClean functionality of Hirschmann BAT-C2. A specially crafted HTTP request can lead to remote code execution in the vulnerable portion of the branch (deletefile). An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.1
CVE-2021-21892	A stack-based buffer overflow vulnerability exists in the Web Manager FsUnmount functionality of Hirschmann BAT-C2. A specially crafted HTTP request can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 9.9
CVE-2021-21894	A directory traversal vulnerability exists in the Web Manager FsTFtp functionality of Hirschmann BAT-C2 A specially crafted HTTP request can lead to arbitrary file overwrite FsTFtp file disclosure. An attacker can make	CVSSv3.1: 9.1

	an authenticated HTTP request to trigger this vulnerability.	
CVE-2021-21895	A directory traversal vulnerability exists in the Web Manager FsTFtp functionality of Hirschmann BAT-C2. A specially crafted HTTP request can lead to FsTFtp file overwrite. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 7.2
CVE-2021-21896	A directory traversal vulnerability exists in the Web Manager FsBrowseClean functionality of Hirschmann BAT-C2. A specially crafted HTTP request can lead to arbitrary file deletion. An attacker can make an authenticated HTTP request to trigger this vulnerability.	CVSSv3.1: 6.5

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	BAT-C2	BAT-C2	08.08.01.00R08 or lower

Solution

Updates are available, which address the vulnerability. Customers are advised to update their product.

Brand	Product Line / Platform	Product	Version
Hirschmann	BAT-C2	BAT-C2	09.12.01.00R01

For Help or Feedback

To view all Belden Security Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.com.

Related Links

- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21872
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21873
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21875
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21876
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21877
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21878
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21879
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21880
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21881
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21882
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21883
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21884
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21885
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21886
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21887
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21888
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21889
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21890
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21891
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21892
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21894
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21895
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21896

Disclaimer

THE SECURITY BULLETIN, AND INFORMATION CONTAINED HEREIN, ARE PROVIDED ON AN "AS IS" BASIS AND DO NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE BULLETIN, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE BULLETIN, IS AT YOUR OWN RISK. INFORMATION IN THIS BULLETIN AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE BULLETINS AT ANY TIME.

Revisions

V1.0 (2022-11-23):	Bulletin created.