https://nciipc.gov.in

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 - 31 Dec 2024 **Vol. 11 No. 24**

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: beyondtrust					
Product: privileged_remote_access					
Affected Version(s): * Up to (including) 24.3.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Dec-2024	9.8	A critical vulnerability has been discovered in Privileged Remote Access (PRA) and Remote Support (RS) products which can allow an unauthenticated attacker to inject commands that are run as a site user. **CVE ID: CVE-2024-12356**	https://www.beyondtrust.com/trust-center/security-advisories/bt24-10	A-BEY-PRIV-070125/1
Product: remote_support					
Affected Version(s): * Up to (including) 24.3.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Dec-2024	9.8	A critical vulnerability has been discovered in Privileged Remote Access (PRA) and Remote Support (RS) products which can allow an unauthenticated attacker to inject commands that are run as a site user. **CVE ID: CVE-2024-12356**	https://www.beyondtrust.com/trust-center/security-advisories/bt24-10	A-BEY-REMO-070125/2
Vendor: classcms					
Product: classcms					
Affected Version(s): * Up to (including) 4.8					
Incorrect Privilege Assignment	16-Dec-2024	4.7	A vulnerability has been found in ClassCMS up to 4.8 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin?do=admin:user:edit Post of the component User Management Page. The manipulation leads to improper handling of insufficient privileges. The attack can be launched remotely. The exploit has been disclosed to the public	N/A	A-CLA-CLAS-070125/3

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and may be used. **CVE ID: CVE-2024-12666**		
Vendor: fabulatech					
Product: usb_over_network					
Affected Version(s): 6.0.6.1					
Improper Resource Shutdown or Release	16-Dec-2024	5.5	A vulnerability classified as problematic has been found in FabulaTech USB over Network 6.0.6.1. Affected is the function 0x22040C in the library ftusbbus2.sys of the component IOCT Handler. The manipulation leads to null pointer dereference. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-12653**	N/A	A-FAB-USB_-070125/4
Improper Resource Shutdown or Release	16-Dec-2024	5.5	A vulnerability classified as problematic was found in FabulaTech USB over Network 6.0.6.1. Affected by this vulnerability is the function 0x220408 in the library ftusbbus2.sys of the component IOCT Handler. The manipulation leads to null pointer dereference. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-12654**	N/A	A-FAB-USB_-070125/5
Improper Resource Shutdown or Release	16-Dec-2024	5.5	A vulnerability, which was classified as problematic, has been found in FabulaTech USB over Network 6.0.6.1. Affected by	N/A	A-FAB-USB_-070125/6

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this issue is the function 0x220420 in the library ftusbbus2.sys of the component IOCT Handler. The manipulation leads to null pointer dereference. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-12655**		
Improper Resource Shutdown or Release	16-Dec-2024	5.5	A vulnerability, which was classified as problematic, was found in FabulaTech USB over Network 6.0.6.1. This affects the function 0x220448 in the library ftusbbus2.sys of the component IOCT Handler. The manipulation leads to null pointer dereference. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-12656**	N/A	A-FAB-USB_-070125/7
Vendor: invoiceplane					
Product: invoiceplane					
Affected Version(s): * Up to (including) 1.6.1					
Insufficient Session Expiration	16-Dec-2024	3.7	A vulnerability was found in InvoicePlane up to 1.6.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /invoices/view. The manipulation leads to session expiration. The attack may be launched remotely. The complexity of	N/A	A-INV-INVO-070125/8

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 1.6.2-beta-1 is able to address this issue. It is recommended to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product. **CVE ID: CVE-2024-12667**		
Vendor: Iobit					
Product: advanced_systemcare_ultimate					
Affected Version(s): * Up to (including) 17.0.0					
Improper Resource Shutdown or Release	16-Dec-2024	5.5	A vulnerability has been found in IObit Advanced SystemCare Utimate up to 17.0.0 and classified as problematic. This vulnerability affects the function 0x8001E000 in the library AscRegistryFilter.sys of the component IOCTL Handler. The manipulation leads to null pointer dereference. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-12657**	N/A	A-IOB-ADVA-070125/9
Improper Resource Shutdown or Release	16-Dec-2024	5.5	A vulnerability was found in IObit Advanced SystemCare Utimate up to 17.0.0 and classified as problematic. This issue affects the function 0x8001E01C in the library AscRegistryFilter.sys of the component IOCTL Handler. The manipulation	N/A	A-IOB-ADVA-070125/10

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to null pointer dereference. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-12658**		
Improper Resource Shutdown or Release	16-Dec-2024	5.5	A vulnerability was found in IObit Advanced SystemCare Utimate up to 17.0.0. It has been classified as problematic. Affected is the function 0x8001E004 in the library AscRegistryFilter.sys of the component IOCTL Handler. The manipulation leads to null pointer dereference. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-12659**	N/A	A-IOB-ADVA-070125/11
Improper Resource Shutdown or Release	16-Dec-2024	5.5	A vulnerability was found in IObit Advanced SystemCare Utimate up to 17.0.0. It has been declared as problematic. Affected by this vulnerability is the function 0x8001E018 in the library AscRegistryFilter.sys of the component IOCTL Handler. The manipulation leads to null pointer dereference. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-IOB-ADVA-070125/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-12660		
Improper Resource Shutdown or Release	16-Dec-2024	5.5	A vulnerability classified as problematic has been found in IObit Advanced SystemCare Utimate up to 17.0.0. This affects the function 0x8001E040 in the library AscRegistryFilter.sys of the component IOCTL Handler. The manipulation leads to null pointer dereference. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-12662**	N/A	A-IOB-ADVA-070125/13
Vendor: ruifang-tech					
Product: rebuild					
Affected Version(s): 3.8.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2024	3.5	A vulnerability, which was classified as problematic, has been found in ruifang-tech Rebuild 3.8.5. This issue affects some unknown processing of the component Project Task Comment Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-12664**	N/A	A-RUI-REBU-070125/14
Improper Neutralization of Input During Web Page	16-Dec-2024	3.5	A vulnerability, which was classified as problematic, was found in ruifang-tech Rebuild 3.8.5. Affected is an unknown function of the	N/A	A-RUI-REBU-070125/15

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			component Task Comment Attachment Upload. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-12665**		
Vendor: Telerik					
Product: ui_for_wpf					
Affected Version(s): * Up to (excluding) 24.4.1213					
Deserialization of Untrusted Data	16-Dec-2024	8.4	In Progress Telerik UI for WPF versions prior to 2024 Q4 (2024.4.1213), a code execution attack is possible through an insecure deserialization vulnerability. **CVE ID: CVE-2024-10095**	https://docs.telerik.com/devtools/wpf/knowledge-base/kb-security-unsafe-deserialization-vulnerability-cve-2024-10095	A-TEL-UI_F-070125/16

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions