

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210813.3 | 13 августа 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Siemens JT2Go and Teamcenter Visualization

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Teamcenter Visualization: before 13.2.0.2 JT2Go: before 13.2.0.2
Дата выявления	9 июня 2021 г.
Дата обновления	9 июня 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-32944	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой использования после освобождения при чтении DGN-файла.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-416: Использование после освобождения</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.8

<p>MITRE: CVE-2021-32936</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально Уязвимость обусловлена ошибкой границ памяти при обработке входных данных в процедуре восстановления DXF-файла.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-787: Запись за границами буфера</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>8.8</p>
<p>MITRE: CVE-2021-32948</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных при чтении DWG-файлов.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-787: Запись за границами буфера</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>8.8</p>

Ссылки на
источники

<https://ics-cert.us-cert.gov/advisories/icsa-21-159-02>
<https://www.cybersecurity-help.cz/vdb/SB2021081108>
<https://www.opendesign.com/security-advisories>