НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221003.18 | 3 октября 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Trend Micro Apex One

Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	Apex One: 2019 - Patch 6 B10048
Дата выявления	13 сентября 2022 г.
Дата обновления	13 сентября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-40139	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой ввода. CVSSv3.0: AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-345: Некорректная проверка достоверности данных Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	9.1

MITRE: CVE-2022-40142 CVE-2022-40143	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код с повышенными привилегиями в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректным разрешением ссылки. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-59: Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке") Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	8.8
MITRE: CVE-2022-40144	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена ошибкой при обработке запросов на аутентификацию. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-287: Некорректная аутентификация Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	7.5

Ссылки на источники	http://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=4553 http://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=4553 http://success.trendmicro.com/jp/solution/000291471 http://success.trendmicro.com/jp/solution/000291471