

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200128.1 | 28 января 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Уязвимость к XSS атаке в ПО Eclipse Memory Analyzer

Идентификатор уязвимости	MITRE: CVE-2019-17634
Идентификатор программной ошибки	CWE-79: Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику выполнить код в целевой системе посредством открытия пользователем специально созданного вредоносного HTML-файла. Уязвимость обусловлена некорректной обработкой специальных HTML символов.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Eclipse Memory Analyzer до v1.9.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	17 января 2020 г.
Дата обновления	24 января 2020 г.
Оценка критичности уязвимости (CVSSv3)	9.0 AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Высокое (H)

Влияние на целостность (I)	Отсутствует (N)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Концептуальное подтверждение (P)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://bugs.eclipse.org/bugs/show_bug.cgi?id=552542